

Citrix® Password Manager-Administratorhandbuch

Citrix Password Manager™ 4.6
Citrix Presentation Server™ 4.5 mit Feature Pack 1, Platinum Edition

Hinweise zu Copyright und Marken

Citrix Password Manager ersetzt die Verschlüsselungsschlüssel bestimmter Endbenutzer bei jedem Wechsel der primären Authentifizierungsmethode, z. B. Ändern des Domänenkennworts oder Ausstellen einer neuen Smartcard. Password Manager kann mit dem optionalen Schlüsselverwaltungsmodul diesen Vorgang automatisch ausführen. Password Manager kann auch die Microsoft Data Protection API (DPAPI) verwenden. Bei Verwendung des optionalen Schlüsselverwaltungsmoduls und/oder von DPAPI kann ein Administrator auf die in Password Manager gespeicherten Anmeldeinformationen des Benutzers für das Unternehmen oder den Privatgebrauch zugreifen, wenn sich der Administrator als dieser Endbenutzer anmeldet. Für zusätzliche Sicherheit wird möglicherweise die Identität der Endbenutzer mit eindeutigen vom Benutzer bereitgestellten Informationen geprüft. Dies stellt ein zusätzliches Sicherheitsniveau für die sekundären Anmeldeinformationen des Benutzers bereit.

Regionale Gesetzesvorschriften zum Benutzercomputing schreiben möglicherweise vor, dass Sie Endbenutzer auf die möglichen Sicherheits- und Datenschutzauswirkungen hinweisen, die eine Bereitstellung des Schlüsselverwaltungsmoduls und der DPAPI-Sicherheitskonfigurationen haben können. Prüfen Sie die Unternehmensrichtlinien und legen Sie fest, welche Benachrichtigung ggf. für die Endbenutzer benötigt wird.

Anerkennung von Marken

Dokumentcode: 30. August 2007 (rcw)

Inhalt

Willkommen

Citrix Password Manager stellt Kennwortsicherheit und Single Sign-On-Zugriff auf Windows-Anwendungen, Webanwendungen und hostbasierte Anwendungen bereit, die in der Citrix Umgebung oder auf dem Desktop ausgeführt werden. Benutzer werden einmal authentifiziert, und Password Manager führt alle anderen Vorgänge aus, d. h. Anmeldung an jedem durch Kennwort geschützten Informationssystem, Einhaltung der Kennwortrichtlinien und Überwachung aller mit Kennwörtern verbundenen Ereignisse. Selbst Endbenutzeraufgaben, u. a. Kennwortänderungen, werden automatisiert.

In diesem Abschnitt wird Folgendes beschrieben:

- „Password Manager-Komponenten“ auf Seite 13
- „Password Manager-Produktlinie“ auf Seite 19
- „Informationen zu diesem Dokument“ auf Seite 23
- „Weitere Informationen und Support“ auf Seite 25

Password Manager-Komponenten

In den folgenden Abschnitten werden die Password Manager-Komponenten beschrieben, die Sie installieren müssen, um Password Manager verwenden zu können. Weitere Informationen finden Sie unter „Planen der Password Manager-Umgebung“ im *Citrix Password Manager-Installationshandbuch*.

Password Manager besteht aus den folgenden Hauptkomponenten:

- Zentraler Speicher
- Password Manager Console
- Password Manager Agent-Software
- Password Manager-Dienst (optional)

Zentraler Speicher

Der zentrale Speicher ist ein zentrales Repository, das in Password Manager zum Speichern und Verwalten von Benutzerdaten und administrativen Daten verwendet wird. Benutzerdaten sind zum Beispiel die Anmeldeinformationen der Benutzer, Antworten auf Sicherheitsfragen und andere auf Benutzer bezogene Daten. Administrative Daten sind zum Beispiel Kennwortrichtlinien, Anwendungsdefinitionen, Sicherheitsfragen und andere allgemeine Daten. Wenn sich ein Benutzer anmeldet, vergleicht Password Manager die Anmeldeinformationen des Benutzers mit den Daten im zentralen Speicher. Wenn der Benutzer kennwortgeschützte Anwendungen oder Webseiten öffnet, werden die entsprechenden Anmeldeinformationen aus dem zentralen Speicher abgerufen.

Password Manager Console

Die Password Manager Console ist das Befehlszentrum von Password Manager. In der Konsole können Sie das Verhalten von Password Manager für die Benutzer anpassen. Hier konfigurieren Sie die Funktionsweise von Password Manager, die bereitgestellten Funktionen, die verwendeten Sicherheitsmaßnahmen und weitere wichtige Einstellungen zum Kennwortschutz.

Die Konsole enthält im linken Bereich vier Objekte oder Knoten. Durch Auswählen eines Knotens werden die Tasks für diesen Knoten angezeigt. Es gibt die folgenden Knoten:

- **Benutzerkonfigurationen**

  Mit diesen Konfigurationen können Sie bestimmte Einstellungen für Benutzer anpassen, die auf den geografischen Standorten oder den Unternehmensrollen der Benutzer basieren. Mit den Einstellungen der anderen drei Knoten werden Benutzerkonfigurationen erstellt.

- **Anwendungsdefinitionen**

  Diese Definitionen stellen die Informationen bereit, damit die Agentsoftware die Anmeldeinformationen der Benutzer an die Anwendungen senden und auftretende Fehlerzustände erkennen kann. Sie können die Anwendungsdefinitionsvorlagen verwenden, die mit Password Manager ausgeliefert werden, um Zeit zu sparen, oder Sie können benutzerdefinierte Definitionen für Anwendungen erstellen, die diese Vorlagen nicht verwenden können. Weitere Vorlagen finden Sie unter:

  http://www.citrix.com/passwordmanager/gettingstarted

- **Kennwortrichtlinien**

  Kennwortrichtlinien steuern die Kennwortlänge, den Typ und die Zeichenvielfalt, die in benutzerdefinierten und automatisch generierten Kennwörtern verwendet werden. In Kennwortrichtlinien legen Sie auch fest, welche Zeichen nicht in Kennwörtern verwendet werden dürfen, und ob alte Kennwörter wieder verwendet werden dürfen. Durch das Erstellen von Kennwortrichtlinien gemäß der Sicherheitsrichtlinien Ihres Unternehmens stellen Sie sicher, dass die Kennwortsicherheit von Password Manager richtig verwaltet wird.

- **Identitätsprüfung**

  Die von Ihnen erstellten Sicherheitsfragen stellen der Agentsoftware ein zusätzliches Sicherheitsniveau bereit, da sie vor Personifikationen und unberechtigten Kennwortänderungen schützen. Benutzer, die sich registrieren und die Sicherheitsfragen beantworten, können die Identität bestätigen, indem sie dieselben Antworten eingeben. Nach der Prüfung können die Benutzer die Self-Service-Tasks für ihr Konto durchführen, z. B. Zurücksetzen des primären Kennworts oder Aufhebung der Kontosperrung. Die Sicherheitsfragen werden auch für die Schlüsselwiederherstellung verwendet.

Password Manager Agent-Software

Password Manager Agent ist die Software, die zur Vermittlung zwischen den Benutzern und den Anwendungen auf den Clientgeräten der Benutzer installiert sein muss.

Wenn ein Benutzer auf eine Anwendung zugreift, die eine Authentifizierung erfordert, fängt die Agentsoftware die Authentifizierungsanfrage der Anwendung ab, sucht die richtigen Anmeldeinformationen und sendet sie an die Anwendung.

Außerdem werden den Benutzern von Password Manager Agent eine Vielzahl von Funktionen bereitgestellt. Welche Funktionen genau den Benutzern zur Verfügung stehen, wird mit den administrativen Einstellungen in den Benutzerkonfigurationen festgelegt. Informationen zu den verfügbaren Einstellungen finden Sie unter „Liste der Password Manager-Einstellungen“ auf Seite 275.

Password Manager Agent bietet die folgenden Funktionen:

- **Symbol im Infobereich**

  Über das Password Manager Agent-Symbol im Infobereich kann auf den Anmeldungsmanager und andere Funktionen von Password Manager zugegriffen werden, z. B. Registrierung der Sicherheitsfragen, Anhalten und Onlinehilfe.

- **Anmeldungsmanager**

  Über die Benutzeroberfläche des Anmeldungsmanagers können Anmeldeinformationen erstellt, angezeigt, bearbeitet und gelöscht werden. Außerdem können die Benutzer über den Anmeldungsmanager die Sicherheitsfragen registrieren und auf die Onlinehilfe zugreifen.

  Auf die meisten Funktionen können die Benutzer über das Menü **Datei** zugreifen:

  - Mit dem Befehl **Neue Anmeldung** können Benutzer Anmeldeinformationen für neue Windows-, web- oder hostbasierten Anwendungen in Password Manager hinzufügen.
  - Über den Befehl **Eigenschaften** können die Benutzer auf die Eigenschaften der Anmeldeinformationen für die jeweilige Anwendung zugreifen. Dort kann der Benutzer das Kennwort, die Benutzer-ID und andere Anmeldeinformationen ändern.
  - Mit dem Befehl **Löschen** können die Anmeldeinformationen des Benutzers für die ausgewählte Anwendung aus dem Anmeldungsmanager gelöscht werden.
  - Mit dem Befehl **Kopieren** werden die ausgewählten Anmeldeinformationen dupliziert. Durch Bearbeiten dieser Kopie kann der Benutzer verschiedene Anmeldeinformationen für eine Anwendung erstellen.

  Außerdem können Sie den Benutzern den Zugriff auf die folgenden Befehle ermöglichen:

  - Mit dem Befehl **Kennwörter anzeigen** im Menü **Ansicht** kann der Benutzer die Kennwörter der im Anmeldungsmanager aufgeführten Anwendungen anzeigen.

    Hinweis: Die Verfügbarkeit dieses Befehls ist von der Einstellung zum Anzeigen von Kennwörtern in der Kennwortrichtlinie abhängig. Wenn Sie nicht möchten, dass die Benutzer das Kennwort für eine Anwendungen anzeigen können, stellen Sie die Kennwortrichtlinie entsprechend ein.

- Mit dem Befehl **Sicherheitsfragenregistrierung** im Menü **Extras** kann der Benutzer den Assistenten für die Sicherheitsfragen-registrierung erneut starten und neue Antworten auf die Sicherheitsfragen angeben.
- Mit dem Befehl **Kontozuordnung** im Menü **Extras** kann der Benutzer Konten in verschiedenen Domänen einander zuordnen. Mit dieser Funktion werden die Anmeldeinformationen des Benutzers synchronisiert und Kennwortänderungen werden domänenübergreifend wirksam.

- **Automatisches Einrichten neuer Anmeldeinformationen**

  Benutzer können mit dem Anmeldungsassistenten schnell neue Anmeldeinformationen erstellen. Password Manager Agent kann erkennen, wann Anmeldeinformationen von einer Anwendung oder Website angefordert werden. Wenn die Anmeldeinformationen des Benutzers nicht bereits in Password Manager gespeichert sind, wird automatisch der Anmeldungsassistent geöffnet, mit dem diese gespeichert werden können.

- **Benutzermobilität**

  Password Manager Agent unterstützt mobile und Remotebenutzer. Wenn ein Remotebenutzer vor dem Trennen der Verbindung eine Lizenz abruft, kann er auch dann auf seine Anmeldeinformationen zugreifen, wenn er nicht mit dem Unternehmensnetzwerk verbunden ist. Mobile Benutzer können zwischen Computern wechseln und mehrere Benutzer können sicher eine Arbeitsstation verwenden.

Password Manager-Dienst

Der Password Manager-Dienst wird auf einem Webserver ausgeführt, der das Fundament für optionale Funktionen bereitstellt, die in diesem Release enthalten sind. Installieren Sie den Password Manager-Dienst, wenn Sie mindestens eines der folgenden Module implementieren möchten:

- Konto-Self-Service: Ermöglicht das benutzerseitige Zurücksetzen der Windows-Kennwörter und das Aufheben der Sperrung der eigenen Windows-Konten.
- Datenintegrität: Schützt die Daten bei der Übertragung vom zentralen Speicher zum Agent vor Manipulation.
- Die Schlüsselverwaltung, mit der Benutzer bei einer Änderung des primären Kennworts die sekundären Anmeldeinformationen wiederherstellen können, entweder mit der automatischen Schlüsselwiederherstellung oder durch das Beantworten von Sicherheitsfragen mit der fragenbasierten Authentifizierung.
- Provisioning: Ermöglicht das Hinzufügen, Entfernen oder Aktualisieren von Benutzerdaten und Anmeldeinformationen von Password Manager in der Konsole.
- Synchronisierung der Anmeldeinformationen: Synchronisiert die Anmeldeinformationen der Benutzer über einen Webdienst.

Wenn Sie die oben angeführten Module nicht implementieren, sollten Sie den Password Manager-Dienst nicht installieren. Weitere Informationen zum Password Manager-Dienst finden Sie unter „Installieren und Konfigurieren des Password Manager-Dienstes“ im *Citrix Password Manager-Installationshandbuch*.

Password Manager-Produktlinie

Password Manager ist jetzt in zwei Editionen erhältlich:

- Password Manager Advanced Edition
- Password Manager Enterprise Edition

Außerdem enthält Citrix Presentation Server 4.5 mit Feature Pack 1, Platinum Edition, eine Funktion „Single Sign-On Powered by Password Manager“, die mit Password Manager Enterprise Edition vergleichbar ist.

Password Manager Advanced Edition

Die Password Manager Advanced Edition erhöht die Sicherheit Ihres Unternehmens durch folgende Funktionen:

- Optionen für starke Kennwortrichtlinien
- Automatische Kennwortgenerierung
- Option zum automatischen Starten des Assistenten für Kennwortänderungen
- Kennwortverschlüsselung bei Speicherzugriff und Übertragung
- Optionen zum Kennwortablauf für Anwendungen ohne entsprechende Funktion

Die Advanced Edition arbeitet auch gut mit anderen Programmen zusammen, wodurch das Speichern der Anmeldeinformationen für den Benutzer und die Verwaltung dieses Vorgangs und dieser Daten für Sie erleichtert wird.

Password Manager Enterprise Edition

Password Manager Enterprise Edition ist für sehr anspruchsvolle und komplexe Unternehmensumgebungen konzipiert. Die Enterprise Edition bietet folgende Vorteile:

- Zusätzliche Sicherheitsfunktionen, Self-Service-Funktionen und Benutzermobilitätsfunktionen für mobile Mitarbeiter im Unternehmen sowie höhere Leistung
- Weniger Helpdeskanrufe durch Self-Service-Funktionen, mit denen die Benutzer ihre Windows-Kennwörter selbst ändern und die Sperrung ihrer Konten selbst aufheben können
- Schneller Zugriff auf Daten für mobile Mitarbeiter im Unternehmen mit Hotdesktop, schnelles Wechseln zwischen Benutzern auf gemeinsam genutzten Arbeitsstationen
- Sicherheitsfunktionen für Unternehmen, wie z. B. Integration von Smartcards, Kerberos und Federated Environment Support (ADFS und SAML).

Vergleich zwischen Password Manager Advanced Edition und Enterprise Edition

Benutzerfunktionen	**Advanced Edition**	**Enterprise Edition**
Single Sign-On für Windows-Anwendungen	X	X
Single Sign-On für Webanwendungen	X	X
Single Sign-On für hostbasierte Terminalemulatoranwendungen	X	X
Citrix Access Client	X	X
Lokalisierte Benutzeroberfläche	X	X
Unterstützung von SAPGUI, Internet Explorer 7 (32 Bit, 64 Bit)	X	X
Benutzerseitige Kennwortrücksetzung		X
Aufheben der Kontosperrung mit dem Self-Service		X
Integration der Self-Service-Funktionen im Webinterface		X
Schneller Wechsel zwischen Benutzern mit Hotdesktop		X
Integration von Hotdesktop/SmoothRoaming		X
Kontozuordnung		X

Sicherheitsfunktionen	Advanced Edition	Enterprise Edition
Automatische Kennwortänderung	X	X
Transparente Kennwortänderung	X	X
Verschlüsselte Kennwörter im Speicher und bei Übertragung	X	X
Richtlinienerzwingung – automatische Kennwortänderungen	X	X
Richtlinienerzwingung – manuelle Kennwortänderungen	X	X
Kennwortablauf	X	X
Unterstützung von Kennworttoken und biometrischer Authentifizierung	X	X
Smartcardunterstützung		X
Kryptografische Sicherung der Datenintegrität	X	X
Kerberos und Federated Environment Support (ADFS, SAML)		X

Administratorfunktionen	Advanced Edition	Enterprise Edition
Provisioning von mehreren Anmeldeinformationen	X	X
Integration mit Produkten für das Provisioning von Anmeldeinformationen	X	X
Unterstützung von Windows NT-Dateifreigaben	X	X
Unterstützung von Microsoft Active Directory	X	X
Unterstützung von Novell Netware-Netzwerkfreigaben	X	X
Unterstützung von LDAP-Verzeichnissen	X	X
Verwaltung mit Active Directory-Gruppen	X	X
Unterstützung von Citrix Streaming Server	X	X
Citrix Access Management Console	X	X
In Platinium Edition integrierte Lizenzierung	X	X
Kompatibilität mit Windows Server 2003 (64 Bit)	X	X
Lizenzierung benannter Benutzer	X	X
CCU-Lizenzierung (nur bei Citrix Password Manager für Presentation Server)		X

Neue Funktionen in Citrix Password Manager 4.6

Citrix Password Manager 4.6 enthält die folgenden neuen Funktionen:

Unterstützung von Windows Vista für Password Manager Agent

Alle Funktionen von Password Manager Agent können jetzt unter Windows Vista verwendet werden. Eine komplette Liste der von Password Manager unterstützten Umgebungen finden Sie unter „Anforderungen für die Password Manager Console und Password Manager Agent“ und „Anforderungen für den Password Manager-Dienst“ im *Citrix Password Manager-Installationshandbuch*.

Verbessertes Provisioning der Anmeldeinformationen

Anmeldeinformationen für Anwendungen können Benutzern jetzt immer bereitgestellt werden, wenn die Password Manager Agent-Software ausgeführt wird. In früheren Versionen konnte das Provisioning nur beim Start der Agentsoftware ausgeführt werden.

Unterstützung mehrerer Domänen für den Dienst

In Password Manager können Sie den Password Manager-Dienst jetzt mit Benutzern anderer Domänen gemeinsam verwenden. Sie installieren die Password Manager Console auf Computern in verschiedenen Domänen und erstellen dann Benutzerkonfigurationen in jeder Domäne.

Maskierte Antworten auf Sicherheitsfragen für die fragenbasierte Authentifizierung

Sie können in Password Manager jetzt die Benutzerantworten auf Sicherheitsfragen der fragenbasierten Authentifizierung maskieren. Wenn die Option aktiviert ist, sind die Antworten der Benutzer bei der Registrierung der Antworten und der Identitätsprüfung geschützt.

Verfügbarkeit des Konto-Self-Service bei gesperrtem Computer

Die Schaltfläche **Konto-Self-Service**, die im Windows-Anmeldedialogfeld angezeigt wird, ist jetzt auch im Dialogfeld **Sperrung des Computers aufheben** verfügbar. Mit dieser Funktion können Benutzer das Netzwerkkennwort zurücksetzen oder die Sperrung der Windows-Domänenkonten aufheben.

Hinweis: Der Konto-Self-Service ist nur in der Enterprise Edition verfügbar.

Informationen zu diesem Dokument

Dieses Handbuch soll Ihnen Folgendes vermitteln:

- Überblick über die Funktionen und Funktionalität von Password Manager
- Anweisungen und Tipps zum Erstellen und Beibehalten der optimalen Kennwortverwaltungsumgebung für die Benutzer

Zielgruppe und Annahmen

Dieses Dokument wendet sich an System- und Sicherheitsadministratoren, die Password Manager implementieren. Grundkenntnisse zur Windows Server-Administration werden vorausgesetzt. Sie müssen mit Novell NetWare vertraut sein, wenn Sie Password Manager auf dieser Plattform installieren oder verwalten.

Feedback zu diesem Handbuch

Um Feedback zur Dokumentation zu geben, gehen Sie auf http://www.citrix.com und klicken Sie auf **Support** > **Knowledge Center** > **Product Documentation**. Klicken Sie auf den Link **Submit Documentation Feedback**, um das Feedbackformular aufzurufen.

Dokumentationskonventionen

Die Citrix Produktdokumentation verwendet die folgenden typografischen Konventionen für Menüs, Befehle, Tasten und Objekte in der Benutzeroberfläche des Programms:

Konvention	Bedeutung
Fettdruck	Befehle, Namen von Benutzeroberflächenobjekten, z. B. Textfelder und Optionsschaltflächen, sowie Benutzereingaben.
Kursiv	Platzhalter für Informationen oder Parameter, die Sie eingeben müssen. *Dateiname* in einem Verfahren bedeutet z. B., dass Sie den tatsächlichen Namen einer Datei eingeben müssen. Außerdem werden neue Begriffe sowie die Titel von Dokumentationen in Kursivschrift angegeben.
%SystemRoot%	Das Windows-Systemverzeichnis, das WTSRV, WINNT, WINDOWS oder ein anderer Verzeichnisname sein kann, den Sie bei der Installation von Windows angegeben haben.
`Nichtproportional`	Text, der in einer Textdatei angezeigt wird.
{geschweifte Klammern}	Eine Reihe von Elementen, von denen eines in Befehlsanweisungen erforderlich ist. Beispiel: **{ ja | nein }** bedeutet, dass Sie entweder **ja** oder **nein** eingeben müssen. Die geschweiften Klammern selbst müssen nicht eingegeben werden.
[eckige Klammern]	Optionale Elemente in Befehlsanweisungen. Beispiel: **[/ping]** bedeutet, dass Sie **/ping** zusammen mit dem Befehl eingeben können. Geben Sie die eckigen Klammern selbst nicht mit ein.
| (vertikaler Strich)	Ein Trennzeichen zwischen Elementen in geschweiften oder eckigen Klammern in Befehlsanweisungen. Beispiel: **{ /hold | /release | /delete }** bedeutet, dass Sie **/hold** oder **/release** oder **/delete** eingeben.
… (Auslassung)	Sie können das vorherige Element bzw. die vorherigen Elemente in Befehlsanweisungen wiederholen. Beispiel: **/route:***Gerätename***[,...]** bedeutet, dass Sie weitere *Gerätenamen*, durch Kommas voneinander getrennt, eingeben können.

Weitere Informationen und Support

In diesem Abschnitt wird die Dokumentation zu diesem Release beschrieben. Außerdem wird beschrieben, wie Sie weitere Informationen zu Password Manager erhalten.

Die folgenden Themen werden behandelt:

- Produktdokumentation
- Kundendienst und technischer Support
- Subscription Advantage
- Schulung und Zertifizierung

Produktdokumentation

Zu Password Manager steht eine umfangreiche Dokumentationsbibliothek zur Verfügung. Die Dokumentation steht auf der Citrix Website (http://www.Citrix.com) zur Verfügung. Direkte Links zur Dokumentation finden Sie in der Datei Password_Manager_Read_Me_First.html im Ordner \Documentation auf der Produkt-CD.

Update-Informationen zur Installation

Die Update-Informationen zur Installation umfassen Informationen zur Installation, die nach Fertigstellung der Readmedatei zusammengestellt wurden. Die Update-Informationen finden Sie unter http://support.citrix.com/article/CTX111284.

Password_Manager_Read_Me_First

Das Dokument Password_Manager_Read_Me_First.html, das auch *Willkommen bei Citrix Password Manager* genannt wird, finden Sie im Order \Documentation auf der Produkt-CD. Das Dokument enthält direkte Links zur Bibliothek der Password Manager-Dokumentation auf der Citrix Website.

Readmedateien

Die Readmedatei enthält Informationen zur Funktionalität von Password Manager, zu bekannten Problemen und Änderungen sowie weitere wichtige Informationen, die nach Fertigstellung des *Citrix Password Manager-Administratorhandbuchs* zusammengestellt wurden. Lesen Sie unbedingt diese Datei, bevor Sie mit der Installation von Password Manager beginnen. Sie befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Handbuch „Schnelleinstieg für die Citrix Lizenzierung“

Die Lizenzierung für Password Manager hat sich seit Password Manager 4.1 geändert. Weitere Informationen zur Lizenzierung von Password Manager finden Sie im Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das auf der Citrix Website und über die Datei Password_Manager_Read_Me_First.html zur Verfügung steht.

Hinweis: Handbücher werden im PDF-Format bereitgestellt. Zum Anzeigen, Durchsuchen und Drucken von PDF-Dokumenten benötigen Sie Adobe Acrobat Reader 5.0.5 mit Acrobat Search oder Adobe Reader 6.0 oder höher. Diese Produkte stehen zum kostenlosen Download auf der Website von Adobe Systems unter http://www.adobe.com bereit.

Citrix Password Manager-Installationshandbuch

Im Citrix Password Manager-Installationshandbuch finden Sie Installations- und Upgradeverfahren für Password Manager. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Citrix Password Manager-Administratorhandbuch

Im Administratorhandbuch (diesem Dokument) finden Sie konzeptionelle Informationen und Anweisungen für Systemadministratoren, die Komponenten von Password Manager verwalten, konfigurieren und testen. Es befindet sich auf der Citrix Website und kann direkt über die Datei Password_Manager_Read_Me_First.html geöffnet werden.

Installationscheckliste

Dieses Dokument ist eine kurze Anleitung für Administratoren, die mit der Installation von Password Manager vertraut sind. Der Installationsvorgang wird sehr grob beschrieben. Die Installationscheckliste ist kein Ersatz für dieses Installationshandbuch. Es befindet sich auf der Citrix Website und kann direkt über die Datei Read_Me_First.html geöffnet werden.

Onlinehilfe für Administratoren und Benutzer

Für Administratoren stehen nun umfangreiche Hilfethemen auf Grundlage des Installations- und Administratorhandbuches bereit. Administratoren können Informationen zu häufigen Aufgaben, Arbeitsabläufen und Einstellungen auf dem Bildschirm anzeigen.

Die Benutzer erhalten Informationen zu häufigen Aufgaben, u. a. zum Erstellen von Anmeldeinformationen für Anwendungen, zum Verwenden des Anmeldungsmanagers und zum Einstellen von automatischen Password Manager-Funktionen. Die Benutzer können die Hilfe über das Menü **Hilfe** oder die Schaltfläche **Hilfe** aufrufen.

Citrix Password Manager Evaluator's Guide

In diesem Handbuch finden Sie einen Überblick über die Funktionen und die Funktionalität von Password Manager. Es enthält Anweisungen zum Einrichten und Ausführen einer kleinen Testumgebung für die Bereitstellung des Produkts.

Kundendienst und technischer Support

Citrix bietet technischen Support hauptsächlich über Citrix Solutions Advisors an. Wenden Sie sich zuerst an Ihren Vertragshändler oder suchen Sie unter http://www.citrix.com nach dem nächstgelegenen Solution Advisor.

Zusätzlich zu Citrix Solution Advisors bietet Citrix zahlreiche Tools zum technischen Onlinesupport und Selbstbedienungssupport im Knowledge Center unter http://support.citrix.com/ an. Das Knowledge bietet Folgendes:

- Eine Knowledge Base mit Tausenden von technischen Lösungen zur Unterstützung der Citrix Umgebung.
- Eine webbasierte Produktdokumentationsbibliothek.
- Interaktive Support-Foren für jedes Citrix Produkt.
- Zugriff auf die neuesten Hotfixes und Service Packs.
- Security Bulletins.
- Webbasierte Problemmeldung und -verfolgung (für Benutzer mit gültigen Supportverträgen).
- Citrix Live Remote Assistance. Mit dem Produkt von Citrix für die Remoteunterstützung, GoToAssist, kann ein Supportmitarbeiter Ihren Desktop sehen und die Maus- und Tastatur zusammen mit Ihnen verwenden, um Ihnen bei der Lösung eines Problems zu helfen.

Eine andere Supportquelle, Citrix Preferred Support Services, bietet eine Reihe von Optionen, sodass Sie den Grad und die Art von Support für die Citrix Produkte in Ihrer Organisation anpassen können.

Subscription Advantage

Subscription Advantage stellt die einfachste und bequemste Möglichkeit dar, Ihre Citrix Software mit den neuesten serverbasierten Funktionen auf dem Laufenden zu halten. Während der Laufzeit des Abonnements erhalten Sie regelmäßig automatisch Folgendes:

- Feature Releases
- Softwareupgrades
- Erweiterungen
- Wartungs-Releases
- Bevorzugten Zugang zu wichtigen technischen Informationen von Citrix

Weitere Informationen zum Abonnement finden Sie auf der Citrix Website unter http://www.citrix.com/services/ (klicken Sie auf **Subscription Advantage**). Weitere Informationen erhalten Sie auch von Ihrem Citrix Vertragshändler oder einem Mitglied von Citrix Solutions Advisors.

Schulung und Zertifizierung

Citrix bietet eine Reihe von unterrichteten (ILT, engl. instructor led training) und webbasierten Kursen (WBT, engl. web-based training). Die von einem Schulungsleiter durchgeführten ILT-Kurse werden von Citrix Authorized Learning Centers (CALCs) angeboten. CALCs bieten hochwertige Schulungen mit den professionellen Schulungsmaterialien von Citrix. Viele diese Kurse bereiten auf eine Zertifizierung vor.

Webbasierte Schulungskurse werden auch von CALCs, Wiederverkäufern und über die Website von Citrix angeboten.

Informationen zu Programmen und Schulungsunterlagen für Citrix Schulungen und Zertifikate finden Sie unter http://www.citrix.com/edu/.

Verwenden von Kennwortrichtlinien zum Erzwingen von Kennwortanforderungen

Mit Citrix Password Manager können Regeln definiert werden, mit denen Sie die Eigenschaften der Kennwörter steuern können, die von den Benutzern gespeichert werden und die für Single Sign-On-aktivierte Anwendungen (SSO) erforderlich sind. Diese Regeln sind die *Kennwortrichtlinien*, die Sie, abhängig vom Unternehmen, auf alle Benutzer oder auf bestimmte Gruppen von Anwendungen anwenden.

In diesem Kapitel wird beschrieben, wie Sie Kennwortrichtlinien in der Password Manager-Umgebung erstellen. Weitere Informationen finden Sie unter „Verwenden von Kennwortrichtlinien für den Zugriff auf Anwendungen“ im *Citrix Password Manager-Installationshandbuch*.

Hinweis: Citrix Presentation Server bietet Richtlinienregeln, mit denen Sie konfigurieren und steuern können, welche Benutzer Password Manager verwenden können, wenn sie sich mit Servern und veröffentlichten Anwendungen in der Serverfarm verbinden. Weitere Informationen finden Sie im *Presentation Server-Administratorhandbuch*.

Kennwortrichtlinien im Überblick

Password Manager enthält zwei Standardkennwortrichtlinien: **Standardrichtlinie** und **Domänenrichtlinie**. Beide Richtlinien können nicht gelöscht werden. Sie können diese Richtlinien unverändert verwenden, kopieren oder ändern, um sie den im Unternehmen geltenden Richtlinien und Vorschriften anzupassen.

Wenn ein Benutzer im Anmeldungsmanager Anmeldeinformationen für eine Anwendung hinzufügt, die nicht von einem Administrator definiert wurde, wird diese Anwendung von Password Manager mit der Standardrichtlinie verwaltet. Wenn Sie eine Anwendungsgruppe als Domänenkennwortgruppe behandeln möchten, müssen Sie die Domänenrichtlinie auf diese Anwendungsgruppe anwenden.

Hinweis: Da Password Manager die Standardrichtlinie auf vom Benutzer hinzugefügte Anwendungen anwendet, sollte die Standardrichtlinie so weit wie möglich gefasst werden, damit Kennwörter für Anwendungen angenommen werden können, für die die Benutzer Kennwörter speichern dürfen.

Sie können im Unternehmen beliebig viele Richtlinien erstellen. So können Sie z. B. eine Richtlinie auf die gesamte Domänengruppe anwenden und einzelne Richtlinien erstellen, die Sie auf einzelne Anwendungsgruppen anwenden, um die Anforderungen weiter zu definieren. Kennwortrichtlinien unterstützen die folgenden Funktionen:

- Automatische Kennwortänderung für Anwendungen.
- Implementieren von Sicherheitsschemas wie komplexe Kennwörter und anwendungsspezifische Kennwörter, die von Benutzern nicht angezeigt werden können.
- Definieren des Kennwortablaufs für Anwendungen, selbst wenn das Kennwort für die Anwendung selbst nicht ungültig wird

---

Hinweis: Wenn Benutzer die Kennwörter ändern, vergleicht Password Manager das alte Kennwort mit dem neuen Kennwort. Mit dieser Option wird verhindert, dass Benutzer identische Kennwörter für dieselbe Anwendung zweimal hintereinander verwenden. Weitere Informationen finden Sie unter „Kennwortverlauf und -ablauf festlegen“ auf Seite 38. Weitere Informationen finden Sie auch unter „Erzwingen von Kennwortrichtlinien“ auf Seite 32.

Kennwortgruppen

Manchmal haben Benutzer ein Kennwort, das für mehrere Anwendungen verwendet wird (z. B. bei einer Produktsuite). Dies wird als *gemeinsame Kennwortverwendung* bezeichnet. Dabei wird dieselbe Authentifizierungsstelle für die Anwendungen verwendet.

Die anderen Anmeldeinformationen für diese Anwendungen (z. B. Benutzername und benutzerdefinierte Felder) können unterschiedlich sein, das Kennwort des Benutzers ist jedoch gleich. Erstellen Sie in diesem Fall eine Anwendungsgruppe, die eine Kennwortgruppe ist. So stellen Sie sicher, dass die Agentsoftware das Kennwort für alle Anwendungen in der Gruppe als Einheit verwaltet. Bei der Änderung des Kennworts in einer Anwendung stellt die Agentsoftware sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe widergespiegelt wird.

Domänenkennwortgruppen

Domänenkennwortgruppen unterscheiden sich von anderen Kennwortgruppen, da das Domänenkennwort des Benutzers als Hauptkennwort für die Anwendungsgruppe verwendet wird. Wenn der Benutzer das Domänenkennwort ändert, stellt die Agentsoftware sicher, dass die Änderung in den Anmelde-informationen für alle anderen Anwendungen in der Gruppe widergespiegelt wird. Es kann nur das Domänenkennwort geändert werden. Benutzer können nur dann Kennwortänderungen für eine der anderen Anwendungen in der Gruppe vornehmen, wenn der Administrator die Anwendung aus der Domänenkennwortgruppe entfernt.

Erzwingen von Kennwortrichtlinien

Password Manager erzwingt die Einhaltung von Kennwortrichtlinien bei Kennwortänderungen, unabhängig davon, ob das Kennwort benutzerdefiniert oder automatisch von Password Manager generiert wurde.

Das Einhalten einer Kennwortrichtlinie wird in den folgenden Situationen nicht erzwungen:

- Ein Benutzer registriert sich bei Password Manager (bei der Erstverwendung)
- Ein Benutzer bearbeitet ein Kennwort im Anmeldungsmanager der Agentsoftware
- Ein Administrator erstellt eine Anwendungsdefinition

Password Manager erzwingt die Einhaltung einer Kennwortrichtlinie auch nicht für bestehende Kennwörter (d. h. Kennwörter, die vor der Password Manager-Implementierung im Unternehmen erstellt wurden), da Benutzern sonst der Zugriff auf bereits verwendete Anwendungen oder Ressourcen verweigert werden könnte.

Erstellen von Kennwortrichtlinien: Assistent für Kennwortrichtlinien

---

Wichtig: Achten Sie beim Erstellen oder Ändern von benutzerdefinierten Kennwortrichtlinien darauf, dass diese zu den Unternehmens- und Anwendungsanforderungen passen. Wenn Sie z. B. eine Richtlinie erstellen, die absolut nicht mit den Anforderungen einer Anwendung übereinstimmt, können sich die Benutzer möglicherweise nicht an dieser Anwendung authentifizieren.

Weitere Informationen zu den Standardeinstellungen für diese Richtlinien finden Sie unter „Standardeinstellungen für die Standardrichtlinie und die Domänenrichtlinie“ im *Citrix Password Manager-Installationshandbuch*. Wenn Sie mit dem Assistenten wie nachfolgend beschrieben eine neue Kennwortrichtlinie erstellen, werden die Einstellungen der Standardrichtlinie von Password Manager verwendet. Sie können die Einstellungen nach Bedarf ändern und die neu erstellte Richtlinie auf die gewünschte Anwendungsgruppe anwenden.

Der Assistent besteht aus den folgenden Seiten:

- „Grundlegende Kennwortregeln festlegen“ auf Seite 34
- „Regeln für Buchstaben festlegen“ auf Seite 35
- „Regeln für Ziffern festlegen“ auf Seite 35
- „Regeln für Sonderzeichen festlegen“ auf Seite 36
- „Ausschlussregeln festlegen (Ausschließen bestimmter Zeichen)“ auf Seite 36
- „Kennwortverlauf und -ablauf festlegen“ auf Seite 38
- „Kennwortrichtlinie testen“ auf Seite 39
- „Anmeldeeinstellungen festlegen“ auf Seite 40
- „Assistent für Kennwortänderungen anpassen“ auf Seite 41

So starten Sie den Assistenten für Kennwortrichtlinien

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Kennwortrichtlinien** aus.
3. Klicken Sie unter **Häufige Tasks** auf **Kennwortrichtlinie erstellen**.

   Der Assistent für Kennwortrichtlinien wird angezeigt.
4. Geben Sie einen Namen und eine Beschreibung für die Kennwortrichtlinie ein und klicken Sie auf **Weiter**.

Grundlegende Kennwortregeln festlegen

Auf dieser Seite können Sie grundlegende Regeln zur Konfiguration der Kennwortlänge und der zulässigen wiederholten Zeichen im Kennwort festlegen.

Kennwortlänge

Geben Sie die Mindestanzahl der erforderlichen Zeichen an. Der Mindestwert ist 0, der Höchstwert ist 128. Stellen Sie sicher, dass die hier eingegebenen Werte den Anforderungen an die Kennwortlänge für Single Sign-On-aktivierte Anwendungen entsprechen.

Zeichenwiederholung in Kennwörtern

- **Höchstanzahl wiederholter Zeichen**

  Der Wert für diese Einstellung muss eine Zahl zwischen 1 und 128 sein. (Der Standardwert ist 6.)

- **Höchstanzahl aufeinanderfolgender gleicher Zeichen**

  Der Wert für diese Einstellung muss eine Zahl zwischen 1 und 128 sein. (Der Standardwert ist 4.) Bei dem Standardwert von 4 ist **aBc1XXXXbb** beispielsweise ein gültiges Kennwort, da **XXXX** viermal hintereinander vorkommt.

Regeln für Buchstaben festlegen

Auf dieser Seite können Sie die Verwendung von Groß- und Kleinbuchstaben für die Kennwörter der Benutzer festlegen. Sie können die folgenden Einstellungen steuern:

- **Kleinbuchstaben zulassen**
    - Erstes Zeichen im Kennwort kann Kleinbuchstabe sein
    - Letztes Zeichen im Kennwort kann Kleinbuchstabe sein
    - Mindestanzahl der Kleinbuchstaben (Standardwert ist 0; Höchstwert ist 128)
- **Großbuchstaben zulassen**
    - Erstes Zeichen im Kennwort kann Großbuchstabe sein
    - Letztes Zeichen im Kennwort kann Großbuchstabe sein
    - Mindestanzahl der Großbuchstaben (Standardwert ist 0; Höchstwert ist 128)

Regeln für Ziffern festlegen

Auf dieser Seite können Sie die Verwendung von Ziffern für die Kennwörter der Benutzer festlegen. Sie können die folgenden Einstellungen steuern:

- **Ziffern zulassen**
    - Erstes Zeichen im Kennwort kann Ziffer sein
    - Letztes Zeichen im Kennwort kann Ziffer sein
    - Mindestanzahl der Ziffern (Standardwert ist 0; Höchstwert ist 128)
    - Zulässige Höchstanzahl der Ziffern (Standardwert ist 20; Höchstwert ist 128)

Regeln für Sonderzeichen festlegen

Auf dieser Seite können Sie die Verwendung von Sonderzeichen (keine Buchstaben und Ziffern) für die Kennwörter der Benutzer festlegen. Sie können die folgenden Einstellungen steuern:

- **Sonderzeichen zulassen**
  - Erstes Zeichen im Kennwort kann Sonderzeichen sein
  - Letztes Zeichen im Kennwort kann Sonderzeichen sein
  - Mindestanzahl der Sonderzeichen (Standardwert ist 0; Höchstwert ist 128)
  - Zulässige Höchstanzahl der Sonderzeichen (Standardwert ist 20; Höchstwert ist 128)
  - Die Liste zulässiger Sonderzeichen enthält die folgenden Zeichen: ! @ # $ ^ & * ( ) _ - + = [ ] \ | ? ,

Ausschlussregeln festlegen (Ausschließen bestimmter Zeichen)

Auf dieser Seite können Sie verhindern, dass bestimmte Zeichen oder Zeichengruppen in Kennwörtern verwendet werden, z. B. geläufige Wörter oder einfach zu erratende Gruppen aufeinander folgender Zeichen, z. B. **abc123** oder **asdfjkl**. Außerdem können Sie die Verwendung von Kennwörtern verhindern, die Teile oder die ganzen Benutzernamen von Windows oder einzelnen Anwendungen enthalten.

- Sie können maximal 256 verschiedene Zeichengruppen angeben, die ausgeschlossen werden.
- Jede Zeichengruppe darf zwischen einem und 32 Zeichen lang sein.
- Bei den Zeichen in den Gruppen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Eine Ausschlussliste, die **abcdefg** enthält, verhindert auch die Verwendung von **AbCDefG** in einem Kennwort.
- Eine Ausschlussliste, die eine Zeichengruppe enthält, z. B. **defg** verhindert auch, dass die Zeichengruppe **abcdefg** verwendet wird.

So erstellen Sie eine Ausschlussliste

1. Klicken Sie auf **Liste bearbeiten**.

   Das Dialogfeld **Ausschlussliste bearbeiten** wird angezeigt.

2. Geben Sie die Zeichen oder Zeichengruppen ein, die nicht in Kennwörtern verwendet werden sollen.

   - Sie können Text aus einem Texteditor mit Kopieren und Einfügen in das Textfeld des Fensters übertragen.
   - Geben Sie in jeder Zeile ein Zeichen bzw. eine Zeichengruppe ein. (Drücken Sie nach jeder Zeile die **Eingabetaste**, um die Einträge voneinander zu trennen.)
   - Jede Gruppe kann maximal 32 Zeichen enthalten.
   - Bei den Zeichen wird nicht zwischen Groß- und Kleinschreibung unterschieden.

3. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Fenster zu schließen.

Um die Kennwörter noch weiter einzuschränken, wählen Sie eine oder beide der folgenden Optionen aus:

- **Anwendungsbenutzername im Kennwort nicht zulassen**

  Wählen Sie diese Option aus, um zu verhindern, dass der vollständige Anwendungsbenutzername im Kennwort verwendet wird.

  Wählen Sie **Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen** aus, um die Verwendung von Teilen des Anwendungsbenutzernamens im Kennwort zu unterbinden. Mit der Option **Zeichenanzahl in Teilen** können Sie festlegen, bei wie vielen eingegebenen Zeichen des Benutzernamens die Verwendung des Kennworts verhindert wird.

  Wenn für diese Option z. B. **4** festgelegt wird, kann kein Kennwort mit den Zeichen **citr**, **trix** oder **itri** verwendet werden, wenn der Benutzername **citrix.4** lautet.

- **Windows-Benutzername im Kennwort nicht zulassen**

  Wählen Sie diese Option aus, wenn Sie verhindern möchten, dass der gesamte Windows-Benutzername im Kennwort verwendet wird.

  Wählen Sie **Teile des Windows-Benutzernamens im Kennwort nicht zulassen** aus, um die Verwendung von Teilen des Windows-Benutzernamens im Kennwort zu unterbinden. Mit der Option **Zeichenanzahl in Teilen** können Sie festlegen, bei wie vielen eingegebenen Zeichen des Benutzernamens die Verwendung des Kennworts verhindert wird.

  Wenn für diese Option z. B. **4** festgelegt wird, kann kein Kennwort mit den Zeichen **citr**, **trix** oder **itri** verwendet werden, wenn der Benutzername **citrix.4** lautet.

Kennwortverlauf und -ablauf festlegen

Auf dieser Seite können Sie die Verwendung neuer Kennwörter erzwingen, wenn alte Kennwörter ablaufen. Der Kennwortverlauf wird für jede von Password Manager verwaltete Anwendung gespeichert.

Wenn Sie diese Option auf eine Anwendung oder Anwendungsgruppe anwenden, werden Kennwortänderungen, die nach der Aktivierung der Richtlinie vorgenommen werden, im Kennwortverlauf des Benutzers gespeichert. Kennwortänderungen, die vor der Aktivierung der Richtlinie vorgenommen werden, werden nicht gespeichert oder zum Verhindern der Wiederverwendung von Kennwörtern verwendet.

Wichtig: Der Kennwortverlauf wird pro Benutzer gespeichert. Wenn Sie die Benutzerdaten für einen Benutzer zurücksetzen, wird der Kennwortverlauf entfernt, und der Kennwortverlauf kann nicht für die gelöschten Kennwörter erzwungen werden.

Kennwortverlauf

- **Neues Kennwort darf nicht mit den alten Kennwörtern identisch sein**

  Wählen Sie diese Option aus, wenn ein neues Kennwort erstellt werden muss, wenn das alte Kennwort des Benutzers abläuft. Sie können auch verhindern, dass Benutzer bis zu 24 bereits in der Password Manager-Umgebung verwendete Kennwörter erneut verwenden.

Kennwortablauf

Hinweis: Die Option für den Kennwortablauf weist Benutzer darauf hin, dass ein Kennwort bald abläuft oder bereits abgelaufen ist. Die Benutzer können abgelaufene Anmeldeinformationen verwenden. Es werden jedoch Erinnerungen für das Ändern des Kennworts oder Aufforderungen zum Ändern des Kennworts angezeigt, bis das Kennwort im Anmeldungsmanager geändert wird.

Mit Anwendungsdefinitionen können Sie ein Skript ausführen, wenn ein Kennwort abläuft. Sie können auch die in Password Manager integrierte Kennwortablaufwarnung verwenden.

Die Einstellungen für den Kennwortablauf in Password Manager sind unabhängig von den Einstellungen für den Kennwortablauf in anderen Softwareanwendungen.

- **Den Anwendungsdefinitionen zugeordnete Einstellungen für Kennwortablauf verwenden**

  Wählen Sie diese Option aus, um die Einstellungen für den Kennwortablauf festzulegen. Diese Einstellungen sind der Anwendungsdefinition zugeordnet, auf die die betreffende Kennwortrichtlinie angewendet wird. Sie können die Anzahl der Tage bis zum Ablauf des aktuellen Kennworts auswählen sowie die Anzahl der Tage, die der Benutzer vor dem Ablauf des Kennworts gewarnt wird.

Kennwortrichtlinie testen

Auf dieser Seite können Sie die Kennwortrichtlinien testen, bevor sie in der Umgebung implementiert werden. Hierdurch wird sichergestellt, dass die Richtlinien wie erwartet funktionieren und den Benutzern genügend Kennwörter zur Verfügung stehen.

Auf der Seite **Kennwortrichtlinie testen** können Sie folgende Funktionen verwenden:

- Klicken Sie auf **Testen**, um ein Kennwort manuell zu überprüfen.
- Klicken Sie auf **Erstellen**, damit von Password Manager ein einzelnes mit der Kennwortrichtlinie kompatibles Kennwort erstellt wird.
- Klicken Sie auf **Mehrere Kennwörter erstellen**, damit von Password Manager eine Liste von Kennwörtern erstellt wird, die den für die betreffende Kennwortrichtlinie definierten Einstellungen entsprechen.

Anmeldeeinstellungen festlegen

Auf dieser Seite können Sie die Agenteinstellungen zum Senden der Anmeldeinformationen und zu Anmeldefehlern steuern.

- **Benutzerseitiges Anzeigen des Kennworts**

  Wählen Sie diese Option aus, damit Benutzer das Kennwort anzeigen können, das den Anwendungen in der Benutzerkonfiguration zugeordnet ist. Mit dieser Option wird gesteuert, ob die Schaltfläche **Anzeigen** im Anmeldungsmanager angezeigt wird.

  Hinweis: Damit die Benutzer die Anwendungskennwörter anzeigen können, müssen Sie die Option **Benutzerseitiges Anzeigen aller Kennwörter im Anmeldungsmanager** in der der betreffenden Kennwortrichtlinie zugeordneten Benutzerkonfiguration aktivieren. Weitere Informationen finden Sie unter „Agentverhalten konfigurieren“ auf Seite 120.

- **Neuauthentifizierung der Benutzer vor dem Senden der Anwendungsanmeldeinfo erzwingen**

  Wählen Sie diese Option aus, wenn Sie erzwingen möchten, dass Benutzer die primären Anmeldeinformationen eingeben müssen, bevor Password Manager Agent die Anmeldeinformationen an eine Anwendung sendet. Diese Einstellung ist für Anwendungen nützlich, die auf vertrauliche Informationen zugreifen, da die Prüfung der Benutzeridentität erzwungen wird.

- **Anzahl der Anmeldewiederholungsversuche**

  Mit dieser Einstellung beschränken Sie, wie oft die Agentsoftware Anmeldeinformationen an eine Anwendung oder Ressource senden kann. Wenn der Wert auf 0 gesetzt ist, wird eine Fehlermeldung beim zweiten versuchten Senden der Anmeldeinformationen angezeigt.

- **Zeitlimit für Wiederholungsversuche**

  Geben Sie die Dauer (in Sekunden) an, in der die Agentsoftware die Anmeldeinformationen nach dem ersten Senden an die Anwendung oder Ressource senden kann. Mit der Einstellung für **Anzahl der Anmeldewiederholungsversuche** legen Sie fest, wie oft die Anmeldung in diesem Zeitraum versucht werden kann.

Assistent für Kennwortänderungen anpassen

Auf dieser Seite können Sie das Verhalten des Assistenten für Kennwortänderungen anpassen. Der Assistent wird gestartet, wenn Benutzer Kennwörter ändern müssen. Der Assistent für Kennwortänderungen reagiert auf Formulare zur Kennwortänderung und führt die Benutzer durch das Verfahren zum Ändern der Kennwörter.

Sie können eine der folgenden Optionen auswählen:

- **Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen**
- **Benutzer können nur ein eigenes Kennwort erstellen**

  Wenn diese Option ausgewählt ist, fordert der Assistent für Kennwortänderungen den Benutzer zur Eingabe eines neuen Kennworts auf.

- **Benutzer können nur ein systemgeneriertes Kennwort auswählen**

  Wenn diese Option ausgewählt ist, verhindert der Assistent für Kennwortänderungen, dass Benutzer ein neues Kennwort eingeben. Stattdessen wird automatisch ein systemgeneriertes Kennwort verwendet.

- **Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden**

  Wenn diese Option ausgewählt ist, sendet der Assistent für Kennwortänderungen automatisch ein systemgeneriertes Kennwort. Der Benutzer sieht möglicherweise das automatische Ausfüllen der Felder des Formulars für die Kennwortänderung sowie die Anzeige der Anwendung, ob die Kennwortänderung erfolgreich war oder fehlgeschlagen ist.

Erhöhen der Kennwortstärke und Steigerung der Sicherheit im Unternehmen

Als Administrator für Password Manager können Sie dazu beitragen, die Stärke der Kennwörter der Benutzer zu erhöhen, indem Sie intelligente Kennwortrichtlinien erstellen. Wie gewohnt müssen Sie dabei die Vorteile einer höheren Kennwortstärke und die einer umfassenden Benutzerfreundlichkeit gegeneinander abwägen.

Berücksichtigen Sie die folgenden Hinweise:

- Voreinstellen von Kennwörtern der Benutzer mit dem Modul **Provisioning**. In diesem Fall brauchen die Benutzer die Kennwörter nicht zu kennen und können sie deshalb nicht unbeabsichtigt anzeigen. Diese Methode erfordert die Koordination zwischen der Benutzerkonfiguration und der zugeordneten Kennwortrichtlinie.
- Legen Sie fest, dass Benutzer die Kennwörter in regelmäßigen Abständen ändern müssen.
- Lassen Sie keine leeren Kennwörter zu.
- Lassen Sie nicht das benutzerseitige Anzeigen des Kennworts zu.
- Stellen Sie sicher, dass Kennwörter nicht erneut verwendet bzw. wiederholt werden.
- Lassen Sie keine Benutzer- oder Anwendungsnamen als Teil des Kennworts zu.
- Setzen Sie durch, dass Benutzer, die regelmäßig auf vertrauliche Informationen zugreifen, stärkere bzw. komplexere Kennwörter haben müssen. Fassen Sie diese Benutzer in Benutzerkonfigurationen zusammen, die die betreffenden Anwendungen enthalten.

Verwenden und Verwalten von Anwendungsdefinitionen

Citrix Password Manager Agent erkennt und reagiert auf Anwendungen auf Grundlage der Einstellungen in *Anwendungsdefinitionen*.

Mit den Formularen, die in den Anwendungsdefinitionen enthalten sind, analysiert die Agentsoftware jede Anwendung beim Start, erkennt bestimmte Identifizierungsmerkmale und stellt fest, ob für die startende Anwendung eine bestimmte Aktion ausgeführt werden muss, z. B.:

- Senden von Anmeldeinformationen des Benutzers bei Anmeldeaufforderung
- Aushandeln einer Oberfläche zum Ändern von Anmeldeinformationen
- Verarbeiten einer Oberfläche zum Bestätigen von Anmeldeinformationen

Anwendungsdefinitionen bestehen aus *Formulardefinitionen* und Konfigurationsoptionen, die für alle Formulare in der Konfiguration gelten. Formulardefinitionen sind Sätze bestimmter Erkennungs- und Aktionsmerkmale von Formularen für Anmeldeinformationen des Benutzers.

In den Einstellungen der Formulardefinition wird erkannt, dass eine Anwendung eine bestimmte Aktion für Anmeldeinformationen des Benutzers anfordert. Außerdem werden die Aktionen definiert, die zum Verarbeiten dieser Anmeldeinformationen erforderlich sind.

Eine Anwendungsdefinition ist eine Sammlung aller Formulare zum Verwalten von Anmeldeinformationen des Benutzers, die einer einzelnen Anwendung zugeordnet sind.

Obwohl die meisten Anwendungen und die entsprechenden Anwendungsdefinitionen nur zwei Formulare zum Verwalten von Anmeldeinformationen des Benutzers verwenden, können beliebig viele Formulare zum Verwalten der Anmeldeinformationen des Benutzers definiert und in einer Anwendungsdefinition enthalten sein.

Password Manager unterstützt eine Vielzahl von Anwendungen, einschließlich Windows-, web- und hostbasierte Anwendungen. Das Programm ist kompatibel mit Java-Anwendungen, SAP-Lösungen und Anwendungen, die auf einem Mainframe-, AS/400-System- oder UNIX-Server gehostet werden.

Auf der Citrix Website (http://www.citrix.com/passwordmanager/gettingstarted) stehen verschiedene vordefinierte Anwendungsdefinitionsvorlagen zur Verfügung, die in Password Manager importiert werden können, um die Anwendungsdefinition zu vereinfachen. Citrix Berater, technische Vertriebsmitarbeiter, Systemintegratoren und Password Manager-Administratoren können auf der Website interaktiv Anwendungsdefinitionen zur Verfügung stellen.

Durch diese gemeinsame Nutzung können Anwendungsdefinitionen mit Single Sign-On-Aktivierung leichter und sicherer implementiert werden. Administratoren sollten bei der Definition von Anwendungsdefinitionen für ihre Umgebung nach Möglichkeit vordefinierte Anwendungsdefinitionsvorlagen verwenden.

Um Anwendungsdefinitionen für Anwendungen zu erstellen, für die keine vordefinierten Anwendungsvorlagen vorliegen, stellt die Supportoberfläche für Anwendungsdefinitionen zwei Programme zur Verfügung: den Assistenten für Anwendungsdefinitionen zum Konfigurieren von Merkmalen, die allen Formularen in der Definition zugeordnet sind, und den Assistenten für Formulardefinitionen, der Administratoren schrittweise anleitet, Unterstützung für Windows-, web- und hostbasierte Anwendungen festzulegen.

Password Manager unterstützt außerdem die externe Anwendungserkennung und Aktionsverarbeitung. Mit dieser Funktion können Implementierer von Drittanbietern die einem Formular zugeordneten Tasks zur Anwendungserkennung und Anmeldeinformationsübertragung erweitern, da während der Anwendungserkennung und Aktionsübertragungsverarbeitung in Password Manager Agent auf externe Prozesse zugegriffen werden kann.

Die Kombination dieser Funktionen ermöglicht Password Manager-Administratoren eine flexible und anpassbare Entwicklungsumgebung für Anwendungsdefinitionen, mit der sie Benutzern einen sicheren und flexiblen Single Sign-On-Zugriff auf wichtige Anwendungen bieten können.

Folgende Themen werden in diesem Kapitel beschrieben:

Anwendungsvorlagen im Überblick

Anwendungsvorlagen sind XML-Dateien, mit denen Sie Anwendungsdefinitionen zwischen verschiedenen Citrix Password Manager-Umgebungen freigeben können. Anwendungsvorlagen verringern den Zeit- und Arbeitsaufwand, da sie ohne größeren Konfigurationsbedarf vom Administrator in Anwendungsdefinitionen umgewandelt werden können. Der Administrator muss zwar bestimmte Informationen für Vorlagen bereitstellen, um die Anwendungsdefinition abzuschließen, die erforderlichen Angaben beschränken sich jedoch in der Regel auf eine URL, den Namen einer ausführbaren Datei, das Ablaufdatum eines Kennworts bzw. andere erweiterte Erkennungseinstellungen.

Anwendungsvorlagen werden mit der Password Manager Console oder dem Anwendungsdefinitionstool installiert. Beide Tools enthalten Anwendungsvorlagen für häufig verwendete Windows- und Webanwendungen.

Weitere Vorlagen finden Sie auf der Citrix Website (http://www.citrix.com/passwordmanager/gettingstarted). Sie können auch selbst Anwendungsvorlagen erstellen und diese dann auf der Website anderen Citrix Administratoren per Upload zur Verfügung stellen.

Wenn für eine Anwendung keine Anwendungsvorlage vorhanden ist, können Sie mit der Password Manager Console oder dem Anwendungsdefinitionstool eine Anwendungsdefinition erstellen. (Weitere Informationen finden Sie unter „Identifizieren von Anwendungen und Ereignissen zum Verwalten von Anmeldeinformationen des Benutzers durch Password Manager Agent“ auf Seite 51.)

Verwalten von Anwendungsdefinitionen mit Vorlagen

Um eine Anwendungsdefinition mit einer Vorlage hinzuzufügen, müssen Sie zuerst sicherstellen, dass die Vorlage in der Password Manager-Umgebung verfügbar ist. Wie bereits beschrieben, sind zahlreiche Anwendungsvorlagen auf der Website verfügbar. Wenn Sie eigene Anwendungsvorlagen erstellt und auf einer Netzwerkfreigabe gespeichert haben, können Sie sie auch von dort importieren.

Nachdem Sie eine Anwendungsvorlage in die Umgebung importiert haben, können Sie damit eine Anwendungsdefinition erstellen. Vorlagen können auch aus Anwendungsdefinitionen erstellt werden. Mit diesen Vorlagen können Sie Anwendungsdefinitionen archivieren oder für andere Password Manager-Administratoren freigeben.

Verwalten Sie Anwendungsdefinitionen mit Vorlagen unter Verwendung der folgenden Vorgehensweisen:

- „Download von Anwendungsvorlagen aus dem Web“ auf Seite 47
- „Importieren von Anwendungsvorlagen von einer Netzwerkfreigabe“ auf Seite 48
- „Hinzufügen einer Anwendungsdefinition mit einer Vorlage“ auf Seite 48
- „Erstellen von Anwendungsvorlagen“ auf Seite 49
- „Exportieren von Anwendungsvorlagen“ auf Seite 50

Download von Anwendungsvorlagen aus dem Web

So downloaden Sie Anwendungsvorlagen von der Citrix Website (http://www.citrix.com/passwordmanager/gettingstarted)

1. Stellen Sie sicher, dass der Knoten **Anwendungsdefinitionen** markiert ist. Wählen Sie im linken Bereich im Anwendungsdefinitionstool bzw. in der Password Manager Console unter **Häufige Tasks** die Option **Vorlagen verwalten** aus, um das Dialogfeld **Vorlagen verwalten** zu öffnen.
2. Wählen Sie den Hyperlink **Anwendungsformulare auf dem Web** aus, um die Webseite für Password Manager-Anwendungsdefinitionen zu öffnen.
3. Wählen Sie die zu importierende Anwendungsvorlage aus.
4. Speichern Sie die XML-Datei der Anwendungsvorlage in einem Verzeichnis, auf das Sie über die Password Manager Console zugreifen können.
5. Klicken Sie nach Abschluss des Downloads auf **Schließen**.
6. Folgen Sie den Anleitungen in „Importieren von Anwendungsvorlagen von einer Netzwerkfreigabe“ auf Seite 48

Importieren von Anwendungsvorlagen von einer Netzwerkfreigabe

So importieren Sie eine Anwendungsvorlage von einer Netzwerkfreigabe

1. Markieren Sie den Knoten **Anwendungsdefinitionen** im linken Bereich des Anwendungsdefinitionstools oder der Password Manager Console und wählen Sie unter **Häufige Tasks** die Option **Vorlagen verwalten** aus, um das Dialogfeld **Vorlagen verwalten** zu öffnen.
2. Klicken Sie auf **Vorlage importieren**.
3. Suchen Sie die XML-Datei der Anwendungsvorlage und klicken Sie auf **Öffnen**. Die importierte Vorlage wird in der Liste im Dialogfeld **Vorlagen verwalten** angezeigt.
4. Führen Sie die Schritte unter „Hinzufügen einer Anwendungsdefinition mit einer Vorlage" auf Seite 48 aus.

Hinzufügen einer Anwendungsdefinition mit einer Vorlage

So fügen Sie eine Anwendungsdefinition mit einer Vorlage hinzu

1. Starten Sie die Anwendung, die Sie definieren möchten.
2. Öffnen Sie die Konsole oder das Anwendungsdefinitionstool auf dem Computer, auf dem die zu definierende Anwendung ausgeführt wird.
3. Klicken Sie im Menü der Konsole auf **Vorgang** oder im Menü des Anwendungsdefinitionstools auf **Datei** und wählen Sie **Anwendungsdefinition erstellen**.
4. Wählen Sie den Anwendungstyp aus, für den eine Anwendungsdefinition erstellt werden soll (Windows, Web oder Host/Mainframe).
5. Wählen Sie **Von Anwendungsvorlage erstellen** aus, um das **Ausgangsformat** festzulegen.
6. Wählen Sie die Vorlage in der Dropdownliste aus. In der Dropdownliste werden Vorlagen für den ausgewählten Anwendungstyp angezeigt.
7. Klicken Sie auf **Assistent starten**.
8. Geben Sie die erforderlichen Informationen ein, um die Anwendungsdefinition abzuschließen. (Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick" auf Seite 53.)
9. Stellen Sie sicher, dass die neue Anwendungsdefinition im Knoten Anwendungsdefinitionen in der Konsole aufgeführt ist.

Sie können eine Anwendungsdefinition auch über das Dialogfeld **Vorlagen verwalten** starten. Dieses Verfahren wird im Folgenden beschrieben.

Erstellen einer Anwendungsdefinition aus einer importierten Vorlage

1. Markieren Sie den Knoten **Anwendungsdefinitionen** im linken Bereich des Anwendungsdefinitionstools oder der Password Manager Console und wählen Sie unter **Häufige Tasks** die Option **Vorlagen verwalten** aus, um das Dialogfeld **Vorlagen verwalten** zu öffnen.
2. Markieren Sie den Namen einer Anwendungsvorlage und klicken Sie auf **Anwendungsdefinition erstellen**. Der Assistent für Anwendungsdefinitionen für den Anwendungstyp, der dieser Vorlage zugeordnet ist. wird gestartet.
3. Geben Sie die erforderlichen Informationen ein, um die Anwendungsdefinition abzuschließen. (Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53.)
4. Stellen Sie sicher, dass die neue Anwendungsdefinition im Knoten Anwendungsdefinitionen in der Konsole aufgeführt ist.

Wenn Sie eine Anwendung ausführen, für die es keine Vorlage gibt, können Sie mit der Password Manager Console oder dem Anwendungsdefinitionstool Anwendungsdefinitionen für diese Anwendung erstellen. (Weitere Informationen finden Sie unter „Identifizieren von Anwendungen und Ereignissen zum Verwalten von Anmeldeinformationen des Benutzers durch Password Manager Agent“ auf Seite 51.) Nach dem Erstellen einer Anwendungsdefinition erstellen Sie eine Vorlage. Diese Vorlage kann exportiert werden, um sie zu archivieren oder per Upload auf die Citrix Website anderen Password Manager-Administratoren zur Verfügung zu stellen (http://www.citrix.com/passwordmanager/gettingstarted).

Erstellen von Anwendungsvorlagen

So erstellen Sie eine Vorlage aus einer vorhandenen Anwendungsdefinition

1. Erweitern Sie den Knoten **Anwendungsdefinitionen** im linken Bereich des Anwendungsdefinitionstools oder der Password Manager Console und wählen Sie die Anwendungsdefinition aus, die Sie zum Erstellen der Vorlage verwenden möchten.
2. Wählen Sie die Option **Als Vorlage speichern** aus, um das Dialogfeld **Als Vorlage speichern** zu öffnen.
3. Um die Vorlage zu archivieren oder sie anderen Password Manager-Administratoren zu Verfügung zu stellen, können Sie die Vorlage in ein XML-Format exportieren. Führen Sie die Schritte unter „Exportieren von Anwendungsvorlagen“ auf Seite 50 aus.

Exportieren von Anwendungsvorlagen

So exportieren Sie eine Vorlage aus einer vorhandenen Anwendungsdefinition

1. Markieren Sie den Knoten **Anwendungsdefinitionen** im linken Bereich des Anwendungsdefinitionstools oder der Password Manager Console und wählen Sie unter **Häufige Tasks** die Option **Vorlagen verwalten** aus, um das Dialogfeld **Vorlagen verwalten** zu öffnen.
2. Markieren Sie die Vorlage in der Liste der verfügbaren Vorlagen und klicken Sie auf **Exportieren**.
3. Definieren Sie den Namen und den Speicherort für die exportierte Vorlagendefinition und klicken Sie auf **OK**. Die exportierte Vorlage wird im angegebenen Verzeichnis gespeichert. Diese Vorlage kann dann zur Sicherung der Daten archiviert bzw. anderen Password Manager-Administratoren zur Verfügung gestellt werden (http://www.citrix.com/passwordmanager/gettingstarted).

Identifizieren von Anwendungen und Ereignissen zum Verwalten von Anmeldeinformationen des Benutzers durch Password Manager Agent

Anwendungsdefinitionen werden mit der Password Manager Console oder dem Anwendungsdefinitionstool erstellt.

Eine Anwendungsdefinition unterstützt sämtliche Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers, die einer Anwendung zugeordnet sind. Dazu gehören:

- Authentifizieren des Benutzers
- Ändern der Anmeldeinformationen des Benutzers
- Bestätigen der Änderungen der Anmeldeinformationen

Beim Erstellen einer Anwendungsdefinition wird der Anwendungstyp beim Starten des Assistenten für Anwendungsdefinitionen identifiziert. Durch den ausgewählten Anwendungstyp wird bestimmt, welche Informationen gesammelt werden.

Anwendungsdefinitionen werden in drei Haupttypen unterteilt:

- Windows-Anwendungen (einschließlich Java-Anwendungen und SAP Logon Pad)
- Webanwendungen (einschließlich Java-Applets)
- Hostanwendungen (mit Zugriff über einen HLLAPI-kompatiblen Terminalemulator)

Anwendungsdefinitionen bestehen aus folgenden Komponenten:

- Anwendungsmerkmale, die für alle Formulare in der Definition gelten. Diese werden über den Assistenten für Anwendungsdefinitionen definiert.
- Formularspezifischen Daten zum Erkennen der einzelnen Ereignisse zum Verwalten von Anmeldeinformationen, die der Anwendung zugeordnet sind. Diese werden über den Assistenten für Formulardefinitionen definiert, der beim Ausführen des Assistenten für Anwendungsdefinitionen gestartet wird.

Die Anwendungsmerkmale für alle Anwendungstypen enthalten ähnliche Konfigurationsinformationen. Die in der Anwendungsdefinition enthaltenen formularspezifischen Daten können jedoch je nach Anwendungstyp stark variieren.

Um eine Anwendungsdefinition zu erstellen, muss der Administrator vom Computer, auf dem die Anwendungsdefinition erstellt wird, auf die Anwendung zugreifen können. Da einige Anwendungssignaturen je nach verwendetem Betriebssystem variieren können, müssen Anwendungsdefinitionen in allen Betriebssystemumgebungen, die im Unternehmen verwendet werden, getestet werden.

Änderungen oder Upgrades einer Anwendung, die nach dem Entwickeln und Bereitstellen einer Anwendungsdefinition vorgenommen werden, müssen stets getestet werden, um zu prüfen, ob die Anwendungsdefinition aufgrund geänderter Anwendungssignaturen modifiziert werden muss.

Identifizieren der Komponenten der Anwendungsbenutzeroberfläche

Die Benutzeroberfläche einer Anwendung umfasst verschiedene Formulare, mit denen anwendungsspezifische Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers verarbeitet werden.

So kann beispielsweise ein Formular zur Eingabe von Anmeldeinformationen, ein zweites zum Ändern eines Anwendungskennworts und ein drittes zum Bestätigen oder Anerkennen einer Änderung der Anmeldeinformationen des Benutzers verwendet werden.

Je nach Typ der zu definierenden Anwendung (Windows, Web oder Host) werden in Password Manager eine Vielzahl unterschiedlicher Kennungen für eine eindeutige Reaktion auf und Identifizierung der Formulare verwendet. Dazu gehören unter anderem der Anwendungstyp, der Fenstertitel und der Dateiname der ausführbaren Datei.

Sobald die Agentsoftware die Anwendung und das Formular erkennt, werden die Benutzer je nach den vorgegebenen Einstellungen dazu aufgefordert, die Anmeldeinformationen bereitzustellen oder zu speichern. Danach werden die gespeicherten Anmeldeinformationen von der Agentsoftware gesendet oder die Benutzer aufgefordert, die Anmeldeinformationen zu aktualisieren.

Assistent für Anwendungsdefinitionen im Überblick

Alle Anwendungsdefinitionen werden mit dem Assistenten für Anwendungsdefinitionen und dem integrierten Assistenten für Formulardefinitionen erstellt.

Um den Assistenten für Anwendungsdefinitionen zu starten, markieren Sie in der Citrix Access Management Console den Knoten **Anwendungsdefinitionen**. Wählen Sie dann unter **Häufige Tasks** den Task **Anwendungsdefinition erstellen** aus.

Die folgenden Informationen werden vom Assistenten für Anwendungsdefinitionen für jeden Anwendungstyp (Windows, Web und Host) gesammelt.

Gesammelte Daten	Windows	Web	Host
Anwendung festlegen	X	X	X
Formulare verwalten	X	X	X
Benutzerdefinierte Felder benennen	X	X	X
Symbol angeben	X		
Erweiterte Erkennung konfigurieren	X	X	X
Kennwortablauf konfigurieren	X	X	X
Einstellungen bestätigen	X	X	X

Anwendung festlegen

Auf dieser Seite wird der Name und eine Beschreibung für die Anwendungsdefinition definiert. Sie können einen beliebigen Namen als Anwendungsnamen definieren.

Beachten Sie dabei Folgendes:

- Mit dem Namen können verschiedene Versionen ein und derselben Anwendung voneinander unterschieden werden.
- Dieser Name wird im zentralen Speicher verwendet.
- Benutzer der Agentsoftware sehen diesen Namen und diese Beschreibung im Anmeldungsmanager.

Formulare verwalten

Die meisten Anwendungen verwenden unterschiedliche Formulare für Anmeldungen und Kennwortänderungen. Außerdem werden von einigen Anwendungen Benutzer mit bestimmten Formularen über erfolgreiche bzw. fehlgeschlagene Kennwortänderungen informiert.

Diese Seite wird verwendet, um der Anwendungsdefinition ein Formular hinzuzufügen. Wählen Sie die Option **Formular hinzufügen** aus, um ein neues Formular hinzuzufügen. Dadurch wird der Assistent für Formulardefinitionen gestartet, mit dem die Formulardaten für ein einzelnes Formular gesammelt werden. Der Assistent für Formulardefinitionen wird für jedes zusätzliche Formular in der Anwendungsdefinition wiederholt. Weitere Informationen finden Sie unter „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.

Nach der Definition eines Formulars sehen Sie im Eigenschaften-Dialogfeld eine Zusammenfassung der Formulareigenschaften, die dem markierten Formular im Bereich **Definierte Anwendungsformulare** zugeordnet sind. Diese Eigenschaften werden auch auf der Seite **Einstellungen bestätigen** des Assistenten für Formulardefinitionen angezeigt.

Benutzerdefinierte Felder benennen

Die Felder für Benutzername und Kennwort gehören in Password Manager zu den Standardinformationen, die für jedes Anmeldeformular angegeben werden müssen. Zusätzlich dazu müssen für einige Anwendungen weitere Informationen wie Datenbankname, Domänenname oder Systemname als Teil der Anmeldeinformationen zur Authentifizierung des Benutzers angegeben werden.

Auf der Seite **Formularaktionen definieren** im Assistenten für Formulardefinitionen können beim Erstellen eines Formulars bis zu zwei benutzerdefinierte Felder hinzugefügt werden. (Weitere Informationen finden Sie unter „Definieren von Formularen“ auf Seite 60.) Wenn Sie beim Erstellen eines Formulars benutzerdefinierte Felder definieren, legen Sie auf dieser Seite den Inhalt des zugeordneten Feldes fest, wenn Benutzer das Formular anzeigen.

Um eine Zugriffstaste für den Namen des benutzerdefinierten Feldes festzulegen, fügen Sie im Feldnamen direkt vor dem zu verwendenden Buchstaben ein kaufmännisches Und-Zeichen (&) ein. Ohne Zugriffstaste legt die Agentsoftware dynamisch einen numerischen Wert als Zugriffstaste für das Steuerelement fest. Diese Ziffer wird auf der Schaltfläche je nach der Anzahl der benutzerdefinierten Felder als (1) oder (2) angezeigt.

Testen Sie das fertige Formular, um sicherzustellen, dass der definierte Name für das benutzerdefinierte Feld nicht zu groß ist.

Symbol angeben

Standardmäßig wird von Password Manager für jeden Anwendungstyp im Anmeldungsmanager ein eigenes Symbol verwendet. Für Windows-Anwendungen kann jedoch ein benutzerdefiniertes Symbol festgelegt werden, damit Benutzer bestimmte Anwendungen im Anmeldungsmanager leichter identifizieren können.

Bedenken Sie, dass bei Verwendung eines benutzerdefinierten Symbols zur Kennzeichnung einer bestimmten Windows-Anwendung der identifizierte Pfad zur Symboldatei für alle Benutzer verfügbar sein muss.

Erweiterte Erkennung konfigurieren

Die Kontrollkästchen zum Konfigurieren der erweiterten Erkennung dienen zum Vermeiden von Schleifen beim Senden bzw. Ändern von Anmeldeinformationen.

Schleifen beim Senden der Anmeldeinformationen

In diesem Szenario können Benutzer, wenn sie sich an einer Anwendung abmelden und zum Anmeldebildschirm zurückkehren, von der Agentsoftware aufgefordert werden, sich erneut anzumelden oder das Anmeldeformular zu ignorieren. Aktivieren Sie das Kontrollkästchen **Nur die erste Anmeldung für diese Anwendung verarbeiten**, wenn Sie nicht automatisch Anmeldeinformationen für nachfolgende Anmeldeformulare senden möchten.

Wenn eine vordefinierte Anwendung das erste Mal gestartet wird und diese Option ausgewählt ist, werden die Anmeldeinformationen bei der ersten Instanz des Anmeldeformulars gesendet, ohne dass ein weiterer Benutzereingriff erforderlich ist. Wenn der Benutzer sich abmeldet und das Anmeldedialogfeld erneut angezeigt wird, wird ungefähr 10 Sekunden lang ein Fenster angezeigt. Der Benutzer hat dann drei Möglichkeiten:

- Fenster schließen: Es werden keine Anmeldeinformationen gesendet.
- Fenster ignorieren: Es werden keine Anmeldeinformationen gesendet.
- Auf den Link klicken: Die Anmeldeinformationen werden gesendet.

Beim Schließen der Anwendung wird die Sitzung beendet und Password Manager sendet die Anmeldeinformationen, wenn die Anwendung das nächste Mal geöffnet wird.

Schleifen beim Ändern der Anmeldeinformationen

In diesem Szenario können Benutzer bei ausgewählter Option **Nur die erste Kennwortänderung für diese Anwendung verarbeiten** aufgefordert werden, nachfolgende Kennwortänderungen zu bestätigen, wenn sie mehrere Male versuchen, beim Zugriff auf eine bestimmte Anwendung das Kennwort zu ändern.

Kennwortablauf konfigurieren

Die Einstellungen und Funktionen für den Kennwortablauf ermöglichen u. a. Folgendes:

- Identifizieren eines Skripts, das beim Kennwortablauf ausgeführt wird (optional)
- Verwenden der Citrix Password Manager-Ablaufwarnung (optional)

Wenn nach Ablauf der *Kennwortrichtlinie*, die dieser Anwendungsdefinition zugeordnet ist, ein Skript ausgeführt werden soll, aktivieren Sie die Option zur Skriptausführung und geben Sie das benutzerdefinierte Skript an, das ausgeführt werden soll. Alle Benutzer müssen auf den Skriptpfad zugreifen können.

Mit diesem benutzerdefinierten Skript können Benutzer aufgefordert werden, Kennwörter für bestimmte oder alle Anwendungen regelmäßig zu ändern oder die Kennwörter automatisch zu ändern, um die Sicherheits- und Gesetzesvorschriften einzuhalten. Diese Prozesse lassen sich auch kombinieren.

In der Regel ruft das Skript eine zugeordnete Anwendung über eine Befehlszeile mit einem Kennwortänderungsparameter oder etwas Ähnlichem auf.

Wahlweise können Sie auch die Option **Citrix Password Manager-Ablaufwarnung verwenden** aktivieren. Beim Aktivieren dieser Option wird eine Warnmeldung zum Ablauf des Citrix Password Manager-Kennworts angezeigt, wenn die Kennwortrichtlinie für die Anwendung angibt, dass das Kennwort abgelaufen ist. Es wird wiederholt eine Meldung angezeigt, dass der festgelegte Zeitraum abgelaufen ist, jedoch keine Änderung des Kennworts erzwungen.

Einstellungen bestätigen

Auf der Seite **Einstellungen bestätigen** können Sie die aktuellen Einstellungen für eine Anwendungsdefinition auf Fehler überprüfen und sie bei Problemen korrigieren, bevor Sie die Konfiguration speichern.

Assistent für Formulardefinitionen im Überblick

Mit dem Assistenten für Formulardefinitionen definieren Sie die Merkmale für die einzelnen Formulare zum Verwalten von Anmeldeinformationen des Benutzers, die in einer Anwendungsdefinition enthalten sein können.

Mit dem Assistenten für Formulardefinitionen wird ein Formular bei der Definition der Anwendung erstmals definiert, wenn Sie den Assistenten für Anwendungsdefinitionen verwenden, ein Formular bearbeiten oder ein Formular einer vorhandenen Anwendungsdefinition hinzufügen.

Mit dem Assistenten für Formulardefinitionen können verschiedene Standardformulare zum Verwalten von Anmeldeinformationen des Benutzers definiert werden, z.B.:

- **Anmeldeformular**

  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.

- **Kennwortänderungsformular**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Formular für eine erfolgreiche Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Formular für eine fehlgeschlagene Kennwortänderung**

  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwortänderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Die Daten, die für jedes Formular gesammelt sind, erfüllen zwei Funktionen:

- Eindeutiges Identifizieren beim Starten eines anwendungsspezifischen Formulars
- Ausführen der erforderlichen Aktionen zum Verarbeiten der Anmeldeinformationen des Benutzers, die dem Formular zugeordnet sind

Alle Formulardefinitionen werden mit dem Assistenten für Formulardefinitionen erstellt, der beim Definieren einer Anwendungsdefinition mit dem Assistenten für Anwendungsdefinitionen initiiert wird. Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53.

Der Assistent für Formulardefinitionen wird über die Seite **Formulare verwalten** des Assistenten für Anwendungsdefinitionen gestartet, wenn Sie auf die Schaltfläche **Formular hinzufügen** klicken.

Die folgende Tabelle enthält die Formularinformationen, die vom Assistenten für Formulardefinitionen für jeden Anwendungstyp (Windows, Web und Host) gesammelt werden.

Gesammelte Daten	**Windows**	**Web**	**Host**
Formular benennen	X	X	X
Formular identifizieren	X	X	X
Formularaktionen definieren	X		
Regeln für Felderkennung einstellen			X
Sonstige Einstellungen konfigurieren	X	X	X
Einstellungen bestätigen	X	X	X

Die Identifizierung von Anwendungsformularen, die eine Aktion erfordern, ist für jeden Anwendungstyp unterschiedlich. Hier finden Sie einen Überblick über die Informationen, die zum Erstellen von Formularen für jeden Anwendungstyp erforderlich sind:

- „Windows-Anwendungsdefinitionen“ auf Seite 59
- „Webanwendungsdefinitionen“ auf Seite 82
- „Host/Mainframe-Anwendungsdefinitionen“ auf Seite 94

Windows-Anwendungsdefinitionen

Mit Windows-Anwendungsdefinitionen werden Windows-Anwendungen, Java-Anwendungen und Anwendungen identifiziert, die über ein SAP Logon Pad gestartet werden.

In der Regel wird jede Anwendung, die mit einer ausführbaren Datei (.exe) gestartet wird, beim Definieren einer Anwendungsdefinition als Windows-Anwendung eingestuft. Windows-Anwendungsdefinitionen werden zum Teil durch Identifizieren von Komponenten der aktiven Anwendung erstellt.

In der Password Manager-Anwendungsdefinition für eine Windows-Anwendung werden Informationen über die Anmeldungsformulare und die Felder, die zum Sammeln von Anmeldeinformationen des Benutzers verwendet werden, mit dem Assistenten für Formulardefinitionen eingegeben.

Der Assistent für Formulardefinitionen wird in folgenden Situationen gestartet:

- Beim Erstellen einer neuen Anwendungsdefinition mit dem Assistenten für Anwendungsdefinitionen
- Beim Bearbeiten eines Formulars in einer vorhandenen Anwendungsdefinition
- Beim Hinzufügen eines Formulars in einer vorhandenen Anwendungsdefinition

Der zu definierende Anwendungstyp wird identifiziert, wenn eine neue Anwendungsdefinition initiiert wird.

Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53 und „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.

Erfassen der erforderlichen Informationen für Windows-Anwendungsdefinitionen

Am besten (und einfachsten) können Sie die für Windows-Anwendungs-definitionen erforderlichen Informationen erfassen, indem Sie die Anwendung starten und zum Formular wechseln, für das ein Ereignis zum Verwalten der Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche oder fehlgeschlagene Kennwortänderung) erforderlich ist, während gleichzeitig der Assistent für Formulardefinitionen über die Konsole oder vom Anwendungsdefinitionstool ausgeführt wird. Der Bildschirmtext des Assistenten enthält Anweisungen dazu, wie Sie die erforderlichen Bestandteile der Anwendung suchen und identifizieren.

Definieren von Formularen

Bei der Formulardefinition werden die formularspezifischen Identifizierungs- und Aktionsinformationen gesammelt. Dabei werden die folgenden Seiten des Assistenten für Formulardefinitionen für Windows-Anwendungen verwendet:

- Formular benennen
- Formular identifizieren
- Formularaktionen definieren
- Sonstige Einstellungen konfigurieren
- Einstellungen bestätigen

Klicken Sie nach Abschluss der Aktionen, die für eine bestimmte Seite erforderlich sind, auf **Weiter**. Die Schaltfläche **Zurück** ist in der Regel auf jeder Seite verfügbar, um zuvor konfigurierte Optionen erneut aufzurufen. Unter Umständen ist es jedoch erforderlich, nachfolgende Einstellungen anzupassen, wenn Sie zuvor konfigurierte Optionen ändern.

Formular benennen

Beim Erstellen von Anwendungsdefinitionen für Windows-Anwendungen wird dem Formular, das erstellt wird, auf der Seite **Formular benennen** des Assistenten für Formulardefinitionen ein benutzerdefinierter Name zugewiesen und der zu erstellende Formulartyp wird identifiziert.

Bedenken Sie, dass der Name, den Sie dem Formular zuweisen, auf der Seite **Formulare verwalten** des Assistenten für Anwendungsdefinitionen angezeigt wird. Weisen Sie daher einen aussagekräftigen Namen für den zu definierenden Formulartyp zu.

Verschiedene Standardformulartypen zum Verarbeiten von Anmelde-informationen des Benutzers können mit dem Assistenten für Formulardefinitionen definiert werden. Dazu gehören:

- **Anmeldung**

  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.

- **Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Erfolgreiche Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Fehlgeschlagene Kennwortänderung**

  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwort-änderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Formular identifizieren

Beim Erstellen von Anwendungsdefinitionen für Windows-Anwendungen werden auf der Seite **Formular identifizieren** die Informationen eingegeben, die erforderlich sind, damit das zu definierende Formular von der Password Manager Agent-Software eindeutig erkannt wird.

Zu diesen Informationen gehören der Fenstertitel und der Name der ausführbaren Datei. Wenn der Name der ausführbaren Datei von der Agentsoftware erkannt wird, wird in der Anwendung nach den definierten Fenstertiteln gesucht.

Wenn ein Fenstertitel erkannt wird, führt die Agentsoftware die für das Formular definierten Aktionen aus.

Sie können die Definition vereinfachen, indem Sie sicherstellen, dass die betreffende Windows-Anwendung gestartet wurde und das Formular für die Anmeldeinformationsaktionen angezeigt wird, die ausgeführt werden sollen (z. B. das Anmeldeformular oder das Formular zur Kennwortänderung).

Klicken Sie auf **Auswählen**, um das betreffende Programm, das bereits auf dem Computer geöffnet ist, zu identifizieren. Dadurch wird das Dialogfeld **Programmfenster auswählen** geöffnet, in dem der Fenstertitel und der Name der ausführbaren Datei für das Formular identifiziert werden.

Im Bereich **Programmfenster** des Dialogfeldes **Programmfenster auswählen** stehen drei Optionen zur Auswahl.

Im Bereich **Programmfenster** werden für jedes identifizierte Programm folgende Informationen angezeigt:

- Fenstertitel
- Name der ausführbaren Datei
- Fensterklasse

Im Bereich **Programmfenster** wird das zu definierende Anwendungsformular in der Liste der Anwendungen, die aktuell auf dem Computer ausgeführt werden, gesucht und ausgewählt. Wenn eine Anwendung ausgewählt wird, wird sie auf dem Bildschirm mit einer Umrandung markiert und kann so leichter identifiziert werden.

Mit zwei Optionen kann die Anzahl der verfügbaren Auswahlen erhöht werden. Wenn die gewünschte ausführbare Datei im System gestartet aber nicht angezeigt ist, aktivieren Sie eins oder beide der folgenden Kontrollkästchen, um zusätzliche Optionen anzuzeigen:

- Ausgeblendete Programmfenster anzeigen
- Untergeordnete Fenster anzeigen

Wählen Sie die dritte Option aus (**Kompletten Pfadnamen der ausführbaren Datei in der Identifizierung (sicherer Pfad) einschließen**), um explizite Pfadangaben zu definieren. Diese sind beim Verwenden von *sicheren Pfaden* erforderlich.

Nach dem Auswählen der Zielanwendung werden auf der Seite **Formular identifizieren** die Informationen basierend auf den ausgewählten Optionen eingetragen.

Zu den Formularkennungen gehören folgende Angaben:

- Fenstertitel für dieses Formular

  Zeigt die Fenstertitel an, die diesem Formular zugeordnet sind.

- Namen und Pfade der ausführbaren Datei

  Zeigt den Namen der ausführbaren Datei und die optionalen Pfadangaben an, die zum Verwenden von *sicheren Pfaden* erforderlich sind.

Fenstertitel für dieses Formular

Der Fenstertitel kann bearbeitet werden, um dynamische Fenstertiteldaten, z. B. eine Datums- oder Sitzungsanzeige, zu verwalten. Zur Unterstützung von dynamischen Daten können sie durch Platzhalterzeichen ersetzt werden, die im Fenstertitel wie folgt angezeigt werden:

Platzhalter	Beschreibung
?	Platzhalter für ein einzelnes Zeichen in dynamischen/sich ändernden Fenstertiteln
*	Platzhalter für dynamische Fenstertiteldaten für ein oder mehrere Zeichen. Dieser Wert empfiehlt sich nicht für leere Fenstertitel. Verwenden Sie in solchen Fällen den Wert NULL.
NULL	Platzhalter für leere Fenstertitel (das Wort NULL muss großgeschrieben sein)

Namen und Pfade der ausführbaren Datei

Im Bereich **Namen und Pfade der ausführbaren Datei** werden der Name der identifizierten ausführbaren Datei und andere Informationen zum *Sicheren Pfad* angezeigt.

Bei sicheren Pfaden werden nur Programminstanzen der Anwendung erkannt, die über die hier definierten Pfade initiiert werden. Wenn mehrere Pfade identifiziert werden, sendet die Agentsoftware nur dann Anmeldeinformationen, wenn das identifizierte Programm über den definierten Pfad ausgeführt wird und alle anderen definierten Formularkennungen vorliegen.

Wenn keine Pfadinformationen definiert sind, wird **Keine Angabe** angezeigt und die Agentsoftware sendet Anmeldeinformationen an jedes Programm, das den anderen Formularkennungen entspricht.

Trennen Sie mehrere Pfade mit Semikolon. Pfade können mit absoluten Pfadangaben oder Umgebungsvariablen identifiziert werden.

Hinweis: Mit Anwendungsdefinitionen, die einen sicheren Pfad enthalten, können Vorlagen für Anwendungsdefinitionen erstellt werden. Der sichere Pfad ist jedoch nicht in der Vorlage enthalten.

Erweiterte Zuordnung

Obwohl die meisten Windows-Formulare mit den Optionen auf der Seite **Formular identifizieren** festgelegt werden können, werden für einige Typen der Formulare erweiterte Zuordnungsoptionen benötigt, die im Dialogfeld **Erweiterte Zuordnung** zur Verfügung stehen. Klicken Sie auf **Erweiterte Zuordnung**, um das Dialogfeld **Erweiterte Zuordnung** anzuzeigen. Weitere Informationen zu diesem Dialogfeld finden Sie unter „Verwenden der erweiterten Zuordnung zum Identifizieren von Windows-Formularen“ auf Seite 67.

Formularaktionen definieren

Auf der Seite **Formularaktionen definieren** können Sie definieren, welche Aktionen von der Agentsoftware ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular gesendet werden können.

Am oberen Seitenrand werden alle Anmeldeinformationen des Benutzers angezeigt, die dem betreffenden Formular zugeordnet sind.

	Anmeldung	**Kennwort-änderung**	**Erfolgreiche Kennwortänderung**	**Fehlgeschlagene Kennwort-änderung**
Benutzername/ID	X	X	X	X
Kennwort	X		X	X
Altes Kennwort		X		
Neues Kennwort		X		
Kennwort bestätigen		X		
Benutzerdefiniertes Feld 1	X		X	X
Benutzerdefiniertes Feld 2	X		X	X
OK	X	X	X	X

Unten auf der Seite wird die definierte Aktionsfolge angezeigt.

Auf dieser Seite werden die Aktionen definiert, die von der Agentsoftware ausgeführt werden, um die erforderlichen Anmeldeinformationen des Benutzers erfolgreich an das identifizierte Formular zu senden.

Für zahlreiche Windows-Anwendungen ist nun folgender Prozess erforderlich:

1. Klicken Sie auf den Hyperlink **Festlegen/Ändern**, der den Anmeldeinformationen eines Benutzers zugeordnet ist. Dadurch wird das Dialogfeld **Steuerelementtext konfigurieren** geöffnet, in dem das Steuerelement identifiziert wird, das die ausgewählten Anmeldeinformationen des Benutzers erhalten soll. Bei bereits geöffnetem Formular enthält dieses Dialogfeld alle möglichen Steuerelemente für den Typ, der dem ausgewählten Wert der Anmeldeinformationen des Benutzers oder Sendeoption zugeordnet ist.

Anmeldeinformationen	Steuerelementtyp
Benutzername/ID	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Kennwort	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Altes Kennwort	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Neues Kennwort	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Kennwort bestätigen	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Benutzerdefiniertes Feld 1	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
Benutzerdefiniertes Feld 2	Bearbeiten, Liste, Kombinationsfeld, Nicht definiert
OK	Schaltfläche. Nicht definiert

   Wenn das Formular der Anmeldeinformationen für die Anwendung nicht geöffnet ist, starten Sie die Anwendung und rufen Sie das richtige Formular für Anmeldeinformationen des Benutzers auf. Wählen Sie dann in diesem Dialogfeld die Option **Wählen Sie ein auf dem Computer ausgeführtes Programm aus** aus, um das Programm auszuwählen. Nach der Auswahl des Anwendungsformulars werden in diesem Dialogfeld die möglichen Steuerelementtypen angezeigt, die den ausgewählten Anmeldeinformationen des Benutzers entsprechen.

2. Wählen Sie den Steuerelementtyp aus, der die Anmeldeinformationen erhalten soll. Bei der Auswahl der verschiedenen möglichen Optionen wird der zugeordnete Steuerelementtyp in der Anwendung markiert, damit der Steuerelementtyp, der die identifizierten Anmeldeinformationen des Benutzers bzw. die Schaltfläche **Senden** erhalten soll, leichter identifiziert werden kann.

3. Wiederholen Sie diese Aktion für alle Anmeldeinformationen des Benutzers, die vom Formular und für die Schaltfläche benötigt werden, um das Formular zu senden.

   Für einige Formulare sind Domänen- oder andere benutzerdefinierte Anmeldeinformationen erforderlich, die erfolgreich gesendet werden müssen, um das Formular zu verarbeiten. Zwei benutzerdefinierte Felder sind verfügbar, um diese Anforderungen zu erfüllen. Weisen Sie diesen Feldern die bestimmten Anmeldeinformationen zu. Die Namen, die diesen Feldern zugeordnet sind, werden auf der Seite **Benutzerdefinierte Felder benennen** im Assistenten für Anwendungsdefinitionen festgelegt (siehe „Assistent für Anwendungsdefinitionen im Überblick" auf Seite 53), wenn das Formular definiert ist.

   Hinweis: Nicht alle Anmeldeinformationen, die oben auf der Seite **Formularaktionen definieren** identifiziert sind, müssen konfiguriert werden.

Nachdem Sie definiert haben, welche Formularfelder die identifizierten Anmeldeinformationen des Benutzers erhalten sollen und welche Schaltfläche zum Senden des Formulars ausgewählt werden soll, ist für viele Windows-Anwendungen die Definition der Formularaktionen abgeschlossen und Sie können mit der nächsten Seite im Assistenten fortfahren.

Für einige Formulare sind jedoch weitere Informationen, Schritte, Sondertasten oder andere Aktionen erforderlich, um einen Task zur Verwaltung der Anmeldeinformationen abzuschließen. Klicken Sie bei diesen Formularen auf **Aktionseditor**, um das Dialogfeld **Aktionseditor** zu öffnen. (Weitere Informationen zum Definieren von Formularaktionen mit dem Aktionseditor finden Sie unter „Definieren der Aktionsfolge für Formulare mit dem Aktionseditor" auf Seite 74.)

Sonstige Einstellungen konfigurieren

Beim Festlegen von Windows-Definitionen geben Sie auf dieser Seite an, ob die Agentsoftware automatisch oder der Benutzer manuell auf die Schaltfläche **Senden** klickt.

Aktivieren Sie das Kontrollkästchen **Agent sendet dieses Formular automatisch**, um das Formular automatisch ohne Benutzereingriff zu senden.

Einstellungen bestätigen

Die Seite **Einstellungen bestätigen** ist die letzte Seite des Assistenten für Formulardefinitionen. Hier können Sie die Konfigurationsoptionen und Einstellungen überprüfen, die dem Formular zugeordnet wurden. Administratoren können auf dieser Seite die Konfiguration überprüfen, bevor sie das Formular beenden und zum Assistenten für Anwendungsdefinitionen zurückkehren, um weitere Formulare zu definieren bzw. um das Bearbeiten einer Anwendungsdefinition abzuschließen.

Verwenden der erweiterten Zuordnung zum Identifizieren von Windows-Formularen

Bei den meisten Windows-Anwendungen kann die Formularidentifizierungszuordnung für Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers auf der Seite **Formulare identifizieren** im Assistenten für Formulardefinitionen festgelegt werden. (Weitere Informationen finden Sie unter „Definieren von Formularen“ auf Seite 83.)

Einige Formulare zum Verwalten von Anmeldeinformationen des Benutzers sind jedoch schwieriger zu identifizieren. Hier reicht es nicht, lediglich die Kombination des Namens der ausführbaren Datei und des zugeordneten Fenstertitels zu bewerten.

Bei diesen Formulartypen können Administratoren im Assistenten für Formulardefinitionen auf der Seite **Formular identifizieren** auf **Erweiterte Zuordnung** klicken, um das Dialogfeld **Erweiterte Zuordnung** zu öffnen.

Das Dialogfeld **Erweiterte Zuordnung** unterstützt folgende Windows-Identifizierungsfunktionen:

- Klasseninformationen
- Steuerelementzuordnung
- SAP-Sitzungsinformationen
- Fensterkennung
- Identifizierungserweiterungen

Klasseninformationen

Diese Einstellung legt die Fensterklassenkennungen fest, die ignoriert bzw. auf die reagiert werden, wenn mehrere Fenster dem angegebenen Fenstertitel und der zugehörigen ausführbaren Datei zugeordnet werden können.

Verwenden Sie diesen Zuordnungstyp nicht für .NET-Anwendungen bzw. für Anwendungen, die die Fensterklasse 32770 (Standardklasse) verwenden.

Diese Einstellung ist bei dynamischen Fensterklassen von Nutzen. Verwenden Sie in diesem Fall Platzhalterzeichen, um eine Kennung für dynamische Fensterklassen zuzuordnen.

Platzhalter	Beschreibung
?	Platzhalter für einzelnes dynamisches/sich änderndes Zeichen.
*	Platzhalter für dynamische Kennungsdaten für ein oder mehrere Zeichen. Dieser Wert empfiehlt sich nicht für leere Fensterklassenkennungen. Verwenden Sie in solchen Fällen den Wert NULL.
NULL	Platzhalter für leere Fensterklassenkennungen (das Wort NULL muss großgeschrieben sein)

Dieses Steuerelement ist auch dann nützlich, wenn Sie versuchen, eine Fensterklasse unter zahlreichen möglichen Fensterklassenzielen zu identifizieren. Es gelten die folgenden Bedingungen:

- Der angegebene Fenstertitel und die zugeordnete ausführbare Datei führen zu mehreren möglichen Entsprechungen. Dieser Fall tritt häufig auf, wenn der Fenstertitel dynamische Daten enthält und Platzhalter angegeben sind.
- Das Zielformular muss einer eindeutigen Fensterklassenkennung zugeordnet sein und für alle anderen möglichen Entsprechungen müssen andere Fensterklassenkennungen gelten.

Wenn Sie Ereignisformulare zum Verwalten von Anmeldeinformationen des Benutzers definieren, die diese Bedingungen erfüllen, werden mit dieser Einstellung die zu ignorierenden und die zulässigen Fensterklassenkennungen identifiziert.

Definieren Sie für Anwendungsdefinitionen, die diese Bedingungen erfüllen, eine Windows-Anwendung, bis die Seite **Formular identifizieren** im Assistenten für Formulardefinitionen angezeigt wird. (Weitere Informationen finden Sie unter „Definieren von Formularen“ auf Seite 83.)

Klicken Sie auf **Erweiterte Zuordnung** und wählen Sie dann die Option **Klasseninformationen** aus. Gehen Sie anschließend wie folgt vor:

1. Klicken Sie auf **Auswählen**, um die Zielanwendung unter den momentan auf dem Computer ausgeführten Anwendungen auszuwählen.

   Hinweis: Um mehr Auswahlmöglichkeiten anzuzeigen, aktivieren Sie das Kontrollkästchen **Ausgeblendete Programmfenster anzeigen** bzw. das Kontrollkästchen **Untergeordnete Fenster anzeigen**. Wenn das Kontrollkästchen **Kompletten Pfadnamen der ausführbaren Datei in der Identifizierung (sicherer Pfad) einschließen** aktiviert ist, wird es ignoriert.

   ---

2. Klicken Sie nach Auswahl der Zielanwendung auf **OK**, um zum Dialogfeld **Erweiterte Zuordnungen** zurückzukehren.
3. Geben Sie im Feld **Diese Fensterklasse ignorieren** die Fensterklasse der zu ignorierenden Fenster ein und im Feld **Fensterklasse zulassen** die Fensterklasse, die die Agentsoftware erkennen soll.
4. Klicken Sie zum Abschluss auf **OK** und fahren Sie mit dem Definieren der Formularaktionen fort. (Weitere Informationen finden Sie unter „Formularaktionen definieren“ auf Seite 64.)

Steuerelementzuordnung

In einigen Anwendungen werden Steuerelementbeschriftungen dynamische Informationen zugewiesen. In diesen Fällen können der Fenstertitel, die ihm zugeordnete ausführbare Anwendung und die Steuerelement-ID(s) für mehrere Formulare zum Verwalten von Anmeldeinformationen des Benutzers identisch sein, während sich die Textbeschriftungen oder andere Eigenschaften auf dem Formular infolge anwendungsspezifischer Ereignisse ändern.

Verwenden Sie für diese Formulartypen die Konfigurationsoptionen zur Steuerelementzuordnung, um ein Formular für eine bestimmte Agentaktion eindeutig zu identifizieren. Dies erfolgt auf der Grundlage eindeutiger Klassen-, Stil- oder Textwerte, die der Steuerelement-ID (bzw. mehreren Steuerelement-IDs, wenn mehrere Definitionen zur eindeutigen Identifizierung des Formulars erforderlich sind) zugeordnet sind.

Definieren Sie für Anwendungsdefinitionen, die diese Bedingungen erfüllen, eine Windows-Anwendung, bis die Seite **Formular identifizieren** im Assistenten für Formulardefinitionen angezeigt wird. (Weitere Informationen finden Sie unter „Definieren von Formularen“ auf Seite 60.)

Klicken Sie auf **Erweiterte Zuordnung** und wählen Sie dann die Option **Steuerelementzuordnung** aus. Gehen Sie anschließend wie folgt vor:

1. Klicken Sie auf **Zuordnung hinzufügen**, um das Dialogfeld **Zuordnungskriterien definieren** zu öffnen.

   Hinweis: Sie müssen lediglich so viele Kriterien zur Steuerelementzuordnung definieren, wie für die Identifizierung des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.

2. Klicken Sie im Dialogfeld **Zuordnungskriterien definieren** auf **Auswählen**, um den Assistenten für Steuerelementzuordnungen zu öffnen.

   Mit diesem Assistenten identifizieren Sie ein Merkmal der Steuerelement-ID (Klasse, Stil oder Text) und den Wert, der vorhanden sein muss bzw. nicht vorhanden sein darf, um das Formular eindeutig zu identifizieren.

3. Wählen Sie die Zielanwendung aus der Liste und klicken Sie auf **Weiter**.

   Hinweis: Aktivieren Sie das Kontrollkästchen **Ausgeblendete Fenster**, um ausgeblendete Fenster anzuzeigen.

   Dadurch werden für jede identifizierte Steuerelement-ID, die für die ausgewählte Anwendung gilt, die Klasse, die Textbeschriftung und die Stileinstellungen angezeigt.

4. Klicken Sie mit der rechten Maustaste auf einen Eintrag zur Steuerelement-ID. Im daraufhin angezeigten Popup können Sie das Merkmal der Steuerelement-ID (Klasse, Stil oder Text) auswählen, mit der das Formular für die ausgewählte Steuerelement-ID qualifiziert werden soll.

5. Wählen Sie das Merkmal aus oder wählen Sie **Keine** aus, um das Popup ohne Auswahl zu schließen. Ein Symbol für das ausgewählte Merkmal wird links neben dem Eintrag angezeigt.

6. Wiederholen Sie die Schritte 4 und 5 für jede Steuerelement-ID, die zur eindeutigen Identifizierung des Formulars verwendet werden soll. Wenn Sie alle Einstellungen ausgewählt und zugewiesen haben, klicken Sie auf **Fertig stellen**, um das Dialogfeld **Zuordnungskriterien definieren** zu schließen.

7. Die Steuerelement-ID und das zugeordnete Merkmal, die zur eindeutigen Identifizierung des Formulars verwendet werden, sind damit identifiziert. Weisen Sie nun jedem Merkmal der Steuerelement-ID einen Wert zu.

   Markieren Sie eine Steuerelement-ID und wählen Sie **Bearbeiten** aus. Im daraufhin angezeigten Dialogfeld **Steuerelementzuordnung definieren** können Sie den Inhalt der ausgewählten Steuerelement-ID bearbeiten. Legen Sie die Variablen für jede Steuerelement-ID so fest, dass sie gleich bzw. ungleich den definierten Werten sein müssen, damit das Formular eindeutig identifiziert wird. Wenn alle Werte definiert sind und ein Zuordnungsname festgelegt wurde, klicken Sie auf **OK** und speichern Sie die Daten.

   Damit kehren Sie zum Dialogfeld **Erweiterte Zuordnung** zurück, in dem die neu definierten Zuordnungswerte für die Steuerelement-ID unter dem soeben definierten Zuordnungsnamen gespeichert sind.

8. Klicken Sie zum Abschluss auf **OK** und fahren Sie mit dem Definieren der Formularaktionen fort. (Weitere Informationen finden Sie unter „Formularaktionen definieren“ auf Seite 64.)

SAP-Sitzungsinformationen

Ältere SAP-Versionen werden über die Standarddefinitionen für Windows- und Webanwendungen verwaltet. Das Dialogfeld **Erweiterte Zuordnung** bietet jedoch Unterstützung für SAP-Anwendungen, bei denen mehrere SAP-Systeme dieselbe SAP GUI-Anmeldebenutzeroberfläche (z. B. SAP Logon Pad) verwenden.

Zum Unterstützen der **SAP-Sitzungsinformationen** muss vom SAP-Administrator das GUI-Skripting auf dem Server aktiviert sein. Dann können die Konsole und die Agentsoftware Daten vom SAP Logon Pad abfragen und die System-ID bzw. den Servernamen bestimmen, die für die eindeutige Identifizierung des bestimmten Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.

Mit der Option **SAP-Sitzungsinformationen** können die Sitzungsinformationen aus einem SAP-Fenster extrahiert werden, um SAP-Anmeldefenster eindeutig zu identifizieren und voneinander zu unterscheiden.

Führen Sie für SAP-Anwendungsdefinitionen, die diese Bedingungen erfüllen, die Definition einer Windows-Anwendung durch, bis die Seite “Formular identifizieren” des Assistenten für Formulardefinitionen angezeigt wird. (Weitere Informationen finden Sie unter „Definieren von Formularen“ auf Seite 60.)

Klicken Sie auf **Erweiterte Zuordnung** und wählen Sie dann die Option **SAP-Sitzungsinformationen** aus. Gehen Sie anschließend wie folgt vor:

1. Stellen Sie sicher, dass die SAP-Anwendung Logon Pad ausgeführt wird.
2. Klicken Sie zum Identifizieren der Zielanwendung auf **Ausgewähltes Fenster verwenden** oder **Anderes Fenster auswählen**.

   Wenn Sie auf **Anderes Fenster auswählen** klicken, wird das Dialogfeld **Programmfenster auswählen** geöffnet. Außerdem werden alle Anwendungen angezeigt, die zurzeit geöffnet sind.

   Hinweis: Die Zielanwendung **SAP Logon Pad** sollte angezeigt sein. Aktivieren Sie keines der in diesem Dialogfeld angezeigten Kontrollkästchen.

   ---

3. Nach dem Auswählen der Anwendung werden die Daten für die SAP-System-ID und den Servernamen automatisch vom Fenster abgerufen. Diese Werte können auch manuell eingegeben werden. Sie können in beiden Feldern reguläre Ausdrücke als Werte verwenden. Dies ist sinnvoll, wenn mehrere Server zugeordnet werden sollen. Ein weiterer Grund für die manuelle Eingabe von Werten ist die Zuordnung von DNS- und NetBIOS-Namen eines Servers. Verwenden Sie das folgende Format, um beides zu unterstützen.

   ```
   ^Servername(\.Domäne\.com)?$
   ```

4. Klicken Sie zum Abschluss auf **OK** und fahren Sie mit dem Definieren der Formularaktionen fort. (Weitere Informationen finden Sie unter „Formularaktionen definieren“ auf Seite 64.)

Hinweis: Über die Funktionen zur Steuerelementzuordnung können Sie ein **Kennwortänderungsformular** identifizieren. (Weitere Informationen finden Sie unter „Steuerelementzuordnung“ auf Seite 69.)

SAP GUI-Skriptingmeldungen können erstellt werden, wenn vom Programm versucht wird, über die SAP GUI eine Verbindung zu SAP Logon Pad herzustellen. In diesem Fall kann durch Ändern einer Registrierungseinstellung vermieden werden, dass die Meldung angezeigt wird.

Der Schlüssel lautet HKEY_CURRENT_USER\Software\SAP\SAPGUI Front\SAP Frontend Server\Security\WarnOnAttach. Dies ist ein DWORD-Wert. Wenn dieser Schlüsselwert auf 0 gesetzt wird, wird die Meldung nicht angezeigt. Der Standardwert ist 1.

Fensterkennung

Auf dieser Seite wird eine Fenstersteuerelement-ID definiert, mit der ein Formular eindeutig identifiziert wird, wenn mehr als ein Fenster identifiziert ist. Dazu wird lediglich der definierte Fenstertitel und der Name der ausführbaren Datei verwendet. Dies ist nur sinnvoll, wenn mit der Fenstersteuerelement-ID zwischen mehreren identifizierbaren Formularen unterschieden werden kann.

Aktivieren Sie das Kontrollkästchen **Zuordnen nach Fenstersteuerelement-ID aktivieren** und geben Sie die Steuerelement-ID an, mit der das zu definierende Formular eindeutig von allen anderen Formularen unterschieden werden kann.

Identifizierungserweiterungen

Identifizierungserweiterungen sind Teil der Anwendungsdefinitions-erweiterungen. Mit diesen Erweiterungen können neben der Agentsoftware externe Anwendungen verwendet werden, um zu erkennen, ob Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers vorliegen und um Anmeldeinformationen zu senden.

Obwohl Password Manager-Administratoren normalerweise Anwendungs-definitionen in der Password Manager Console und im Anwendungsdefinitions-tool erstellen, sind für einige Anwendungen aufgrund spezieller Anforderungen alternative Verfahren erforderlich, um die Anwendung zu erkennen und Anmeldeinformationen des Benutzers zu senden bzw. ähnliche Aktionen auszuführen.

Um diese Anwendungen zu unterstützen, können Password Manager-Administratoren mit Anwendungsdefinitionserweiterungen eine Abstraktion für die Anwendungssteuerelemente und die zugeordneten Dateneingabemechanismen schaffen.

Identifizierungserweiterungen werden von Implementierern von Drittanbietern entwickelt. Die Implementierung erfolgt anwendungsspezifisch. Aus diesem Grund sind die erforderlichen Verfahren zum Konfigurieren ihrer Verwendung ebenfalls anwendungsspezifisch.

Im Allgemeinen sind Password Manager-Administratoren nicht an der Entwicklung dieser Erweiterungen beteiligt. Erweiterungen werden von Implementierern von Drittanbietern erstellt. Da die Konfiguration dieser Erweiterungen erweiterungsspezifisch ist, sind der Erweiterung in der Regel Konfigurationsanleitungen beigefügt.

Weitere Informationen finden Sie unter „Erweiterungen von Anwendungsdefinitionen“ auf Seite 313.

Definieren der Aktionsfolge für Formulare mit dem Aktionseditor

Auf der Seite **Formularaktionen definieren** können Sie definieren, welche Aktionen von der Agentsoftware ausgeführt werden müssen, damit die Anmeldeinformationen für das zu definierende Formular zum Verwalten von Anmeldeinformationen des Benutzers gesendet werden können. Für zahlreiche Windows-Anwendungen ist nur der unter „Formularaktionen definieren“ auf Seite 64 beschriebene Prozess erforderlich.

Für einige Formulare sind jedoch weitere Informationen, Schritte, Sondertasten oder andere Aktionen erforderlich, um einen Task zum Verwalten von Anmeldeinformationen des Benutzers abzuschließen. Klicken Sie für diese Formulare auf **Aktionseditor** (im Dialogfeld “Formularaktionen definieren”), um das Dialogfeld **Aktionseditor** zu öffnen.

Im Dialogfeld **Aktionseditor** wird Folgendes angezeigt:

- Verfügbare Aktionen

  Zur Anzeige aller verfügbaren Aktionsfolgeaktionen:

- Aktionskonfiguration

  Zur Definition der aktionsspezifischen Optionen in der Aktionsfolge.

- Aktionsfolge

  Zur Anzeige der Reihenfolge, in der definierte Aktionen ausgeführt werden müssen, um das spezifische Formular zum Verwalten von Anmeldeinformationen des Benutzers zu verarbeiten.

Unten im Dialogfeld **Aktionseditor** wird die Schaltfläche **Erweiterte Einstellungen** anzeigt, mit der das Dialogfeld **Erweiterte Einstellungen** aufgerufen wird. Das Dialogfeld **Erweiterte Einstellungen** hat zwei Steuerelemente:

- **Ordinalzahlen für Steuerelemente**

  Aktivieren Sie dieses Kontrollkästchen, um keine Steuerelement-ID-Nummern sondern Ordinalzahlen für Steuerelemente (häufig als Z-Reihenfolge bezeichnet) zu verwenden. Ordinalzahlen für Steuerelemente werden bei der Definition unabhängig (und von der Agentsoftware) festgelegt, um die Steuerelemente unabhängig von den Steuerelement-ID-Nummern, die von der Anwendung definiert werden, eindeutig zu identifizieren.

  Die Auswahl dieser Funktion wird bei der Definition von .NET-Anwendungen, die dynamische Nummern für Steuerelement-IDs generieren, oder für Anwendungen mit duplizierten Nummern für Steuerelement-IDs empfohlen.

- **Anfängliche Verzögerung**

  Wählen Sie diese Option aus und definieren Sie, wie lange die Agentsoftware wartet, bevor die Aktionsfolge initiiert wird. Die Verzögerungsfunktion kann hier oder über die Aktion **Verzögerung einfügen** beim Starten der Aktionsfolge konfiguriert werden. (Weitere Informationen finden Sie unter „Aktionsbeschreibungen“ auf Seite 77.)

  Im Gegensatz zur Option **Verzögerung einfügen** im Bereich **Verfügbare Aktionen** des Dialogfelds **Aktionseditor**, die als SendKeys-Vorgang definiert wird, wird mit jeder hier definierten anfänglichen Verzögerung vermieden, dass die erstellte Anwendungsdefinition nur von den Versionen 4.5 und 4.6 der Agentsoftware unterstützt wird.

Definition der Aktionsfolge

Die Definition besteht aus den folgenden Schritten:

1. Wählen Sie unter **Verfügbare Aktionen** eine Aktion aus.
2. Konfigurieren Sie die Aktion mit den Optionen zur **Aktionskonfiguration**. Wenn Sie die gewünschten Konfigurationseinstellungen ausgewählt haben, klicken Sie auf **Einfügen**. Die konfigurierte Aktion wird unter **Aktionsfolge** angezeigt.
3. Wiederholen Sie die Schritte 1 und 2 für alle Aktionen, die für das Formular für Anmeldeinformationen des Benutzers erforderlich sind.
4. Markieren Sie die Aktionen und klicken Sie auf **Auf** oder **Ab**, um die Aktionen in der Reihenfolge anzuordnen, die für das zu definierende Formular zum Verwalten von Anmeldeinformationen des Benutzers erforderlich ist.
5. Wenn die Aktionsfolge richtig und vollständig ist, klicken Sie auf **OK**. Dadurch kehren Sie zur Seite **Formularaktionen definieren** zurück, auf der die definierte Aktionsfolge dann im Bereich **Aktionsfolge** angezeigt wird.
6. Klicken Sie auf **Weiter**, um mit der Definition des Formulars auf der Seite **Sonstige Einstellungen konfigurieren** fortzufahren. Wenn die definierte Aktionsfolge aufgrund der verwendeten Kombination von Formularaktionen auf die Versionen 4.5 oder 4.6 der Agentsoftware beschränkt ist, wird eine Meldung angezeigt, in der Sie auswählen können, ob Sie fortfahren oder die Konfiguration ändern möchten.

Aktionsbeschreibungen

In den folgenden Aktionsbeschreibungen wird jede Aktion als Steuerelement-ID-Vorgang, SendKeys-Vorgang (zum Imitieren einer Tastatureingabe) oder erweiterter Vorgang identifiziert. Vermeiden Sie das Erstellen von Anwendungsdefinitionen, die nicht von den Versionen 4.0 und 4.1 der Agentsoftware unterstützt werden, indem Sie Aktionsfolgen identifizieren, die nur Steuerelement-ID-Vorgänge bzw. nur SendKeys-Vorgänge enthalten. In den Versionen 4.0 und 4.1 von Password Manager Agent werden keine Aktionsbeschreibungen unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Aktionsbeschreibungen enthalten.

Steuerelementtext festlegen (Steuerelement-ID-Vorgang)

Mit der Aktion **Steuerelementtext festlegen** werden Anmeldeinformationen des Benutzers den Zielfenster-Steuerelementen auf dem Formular zugewiesen. In der Liste werden nur Anmeldeinformationen des Benutzers angezeigt, die nicht zugewiesen sind.

Bei Auswahl dieser Option werden alle bearbeitbaren Steuerelemente im ausgewählten Formular angezeigt.

Wenn ein Fenstersteuerelement ausgewählt ist, wird das zugeordnete Steuerelement in der Anwendung markiert. So können Sie einem Steuerelement leichter die richtigen Anmeldeinformationen des Benutzers zuweisen.

Um einem Steuerelement einen Wert zuzuweisen, wählen Sie einen Wert unter **Anmeldeinformationen des Benutzers** und das ihm zugeordnete **Fenstersteuerelement** aus und klicken Sie auf **Einfügen**.

Formular senden

Mit der Aktion **Formular senden** ordnen Sie eine Sendeaktion einer Schaltfläche zu. Für dieses Aktionssteuerelement sind zwei Optionen verfügbar: Auf eine Fensterschaltfläche klicken (Steuerelement-ID-Vorgang) oder Eingabetaste senden (SendKeys-Vorgang).

Klicken Sie auf die Schaltfläche **Auf eine Fensterschaltfläche klicken**, um die Schaltfläche auf dem Formular der Sendeaktion zuzuordnen.

Wenn eine Fensterschaltfläche ausgewählt ist, wird das zugeordnete Steuer-element in der Anwendung markiert. So können Sie einem Steuerelement leichter die richtigen Anmeldeinformationen des Benutzers zuweisen.

Klicken Sie zum Abschluss der Auswahl auf **Einfügen**.

Text an Fenster senden (SendKeys-Vorgang)

Mit der Aktion **Text an Fenster senden** senden Sie Text oder Anmelde-informationen des Benutzers als SendKeys-Vorgang an das Formular. Beim Senden von Anmeldeinformationen des Benutzers werden nur nicht zugewiesene Werte in der Liste angezeigt. Klicken Sie zum Abschluss der Auswahl auf **Einfügen**.

Tastenkombination senden (SendKeys-Vorgang)

Mit der Aktion **Tastenkombination senden** senden Sie eine beliebige Kombination aus Tastenmodifikator und ausgewählter Taste an das Formular. Klicken Sie zum Abschluss der Auswahl auf **Einfügen**.

Sondertaste senden (SendKeys-Vorgang)

Mit der Aktion **Sondertaste senden** senden Sie eine Sondertaste an das Formular. Um einen Wert an das Formular zu senden, wählen Sie unter **Kategorie** und **Taste** einen Wert aus und klicken Sie auf **Einfügen**.

Verzögerung einfügen (SendKeys-Vorgang)

Mit der Aktion **Verzögerung einfügen** legen Sie eine Zeitdauer fest, bevor die nächste Aktion in der Aktionsfolge verarbeitet wird.

Um eine Verzögerung einzufügen, geben Sie einen Wert unter **Verzögerung** ein und klicken Sie auf **Einfügen**.

Aktionserweiterung starten (Erweiterter Vorgang)

Aktionserweiterungen sind Teil der Anwendungsdefinitionserweiterungen. Mit diesen Erweiterungen können neben der Agentsoftware externe Anwendungen verwendet werden, um zu erkennen, ob Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers vorliegen und um Anmeldeinformationen zu senden.

Obwohl Password Manager-Administratoren normalerweise Anwendungsdefinitionen in der Password Manager Console und im Anwendungsdefinitionstool erstellen, sind für einige Anwendungen aufgrund spezieller Anforderungen alternative Verfahren erforderlich, um die Anwendung zu erkennen und Anmeldeinformationen des Benutzers zu senden bzw. ähnliche Aktionen auszuführen.

Um diese Anwendungen zu unterstützen, können Password Manager-Administratoren mit Anwendungsdefinitionserweiterungen eine Abstraktion für die Anwendungssteuerelemente und die zugeordneten Dateneingabemechanismen schaffen.

Die von Drittanbieter-Implementieren entwickelten Erweiterungen sind anwendungsspezifisch. Aus diesem Grund sind die erforderlichen Verfahren zum Konfigurieren ihrer Verwendung ebenfalls anwendungsspezifisch.

Im Allgemeinen sind Password Manager-Administratoren nicht an der Entwicklung dieser Erweiterungen beteiligt. Erweiterungen werden von Implementierern von Drittanbietern erstellt. Da die Konfiguration dieser Erweiterungen erweiterungsspezifisch ist, sind der Erweiterung in der Regel Konfigurationsanleitungen beigefügt.

Weitere Informationen finden Sie unter „Erweiterungen von Anwendungsdefinitionen“ auf Seite 313.

Überlegungen für Windows-Anwendungsdefinitionen

Beachten Sie beim Definieren von Windows-Anwendungsdefinitionen die folgenden Punkte:

- Anwendungsvorlagen erleichtern das Erstellen von Anwendungsdefinitionen. Citrix bietet Anwendungsvorlagen für zahlreiche häufig verwendete Anwendungen. Wenn die gesuchte Vorlage nicht Bestandteil des installierten Produkts ist, können Sie prüfen, ob sie auf der Citrix Website (http://www.citrix.com/passwordmanager/gettingstarted) verfügbar ist. Weitere Informationen finden Sie unter „Anwendungsvorlagen im Überblick“ auf Seite 46.
- Testen Sie die Anwendungsdefinitionen mit der Agentsoftware, bevor Sie sie Benutzern zur Verfügung stellen.
- Von den meisten Anwendungsdefinitionen werden nur die grundlegenden Informationen verwendet. Wenn eine Anwendungsdefinition in der Testumgebung nicht wie erwartet funktioniert, kann dies auf eindeutige Funktionen wie dynamische Fenstertitel, dynamische Steuerelement-IDs oder andere spezielle Kennungen oder Aktionen zurückzuführen sein, die in die Anwendung programmiert wurden.
- Mit dem Task **Administrative Daten exportieren** in der Password Manager Console können Sie Anwendungsdefinitionen aus der Testumgebung in die Produktionsumgebung exportieren.
- Einstellungen, die auf Anwendungsdefinitionsebene ausgewählt sind, gelten für alle Formulare innerhalb der Anwendungsdefiniton.
- Einige Einstellungen, die auf Anwendungsdefinitionsebene ausgewählt sind, können jedoch auf Formularebene überschrieben werden. Für eine Anwendung mit drei definierten Formularen kann beispielsweise auf Anwendungsdefinitionsebene das automatische Senden aktiviert werden. Jedes Mal, wenn die Agentsoftware auf eines dieser drei Formulare für diese Anwendung trifft, werden die Anmeldeinformationen des Benutzers automatisch bereitgestellt und gesendet. Das automatische Senden kann jedoch auf Formularebene für eines der Formulare deaktiviert werden, sodass die Agentsoftware die Informationen für dieses bestimmte Formular nicht automatisch sendet. In diesem Fall muss der Benutzer für das ausgewählte Formular auf **Senden** oder **OK** klicken.

- Um eine Zugriffstaste für den Namen des benutzerdefinierten Feldes festzulegen, fügen Sie im Feldnamen direkt vor dem zu verwendenden Buchstaben ein kaufmännisches Und-Zeichen (&) ein.

  Ohne Zugriffstaste legt die Agentsoftware dynamisch einen numerischen Wert als Zugriffstaste für das Steuerelement fest. Diese Ziffer wird auf der Schaltfläche je nach der Anzahl der benutzerdefinierten Felder als (1) oder (2) angezeigt.

  Testen Sie das fertige Formular, um sicherzustellen, dass der definierte Name für das benutzerdefinierte Feld nicht zu groß ist.

- Password Manager speichert Anwendungsdefinitionen in den folgenden Dateien:

  - applist.ini: Diese Datei enthält die von Citrix bereitgestellten Anwendungsvorlagen.
  - entlist.ini: Diese Datei enthält die von Ihnen erstellten Anwendungsdefinitionen.
  - aelist.ini: Diese Datei enthält die benutzerdefinierten Einträge aus entlist.ini und die Einträge aus applist.ini. Durch die Kombination der beiden Dateien in einer Datei erhalten Sie eine vollständige Liste der in der Agentsoftware verfügbaren Anwendungsdefinitionen. Die Agentsoftware überschreibt aelist.ini, wenn eine Synchronisierung mit dem zentralen Speicher erfolgt, z. B. beim Start der Agentsoftware, und verwendet die Datei zur Erkennung bekannter Anwendungen.

Hinweis: Bearbeiten Sie die Datei applist.ini nicht direkt. Zukünftige Releases von Password Manager können die Änderungen an der Datei applist.ini überschreiben. Die angepasste INI-Datei erhält dann die Erweiterung .bak, und die Agentsoftware verwendet statt der geänderten Datei die aktualisierte Datei. Statt die Datei applist.ini zu bearbeiten, sollten Sie stets mit der Konsole festlegen, welche Anwendungen von der Agentsoftware erkannt werden.

Webanwendungsdefinitionen

Mit Webanwendungsdefinitionen werden webbasierte Anwendungen, einschließlich Java-Applets, identifiziert.

In der Regel wird jede Anwendung, die in einem Browser ausgeführt wird, beim Definieren einer Anwendungsdefinition als Webanwendung eingestuft. Password Manager unterstützt Webanwendungen, die mit Internet Explorer Version 6.0 bzw. 7.0 ausgeführt werden.

Webanwendungsdefinitionen werden zum Teil durch Identifizieren von Teilen der aktiven Webanwendung erstellt.

In der Password Manager-Anwendungsdefinition für eine Webanwendung werden Informationen über die Anmeldungsformulare und die Felder, die zum Sammeln von Anmeldeinformationen des Benutzers verwendet werden, mit dem Assistenten für Formulardefinitionen eingegeben.

Der Assistent für Formulardefinitionen wird in folgenden Situationen gestartet:

- Beim Erstellen einer neuen Anwendungsdefinition mit dem Assistenten für Anwendungsdefinitionen
- Beim Bearbeiten eines Formulars in einer vorhandenen Anwendungsdefinition
- Beim Hinzufügen eines Formulars zu einer vorhandenen Anwendungsdefinition

Der Anwendungstyp wird identifiziert, wenn eine neue Anwendungsdefinition erstellt wird.

Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53 und „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.

Erfassen der erforderlichen Informationen für Webanwendungsdefinitionen

Am besten (und einfachsten) können Sie die für Webanwendungsdefinitionen erforderlichen Informationen erfassen, indem Sie die Anwendung starten und zum Formular wechseln, für das ein Ereignis zum Verwalten der Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) erforderlich ist, während gleichzeitig der Assistent für Formulardefinitionen in der Konsole oder vom Anwendungsdefinitionstool ausgeführt wird. Der Bildschirmtext des Assistenten enthält Anweisungen zum Suchen und Identifizieren der erforderlichen Bestandteile der Anwendung.

Definieren von Formularen

Bei der Formulardefinition werden die formularspezifischen Identifizierungs- und Aktionsinformationen gesammelt. Dabei werden die folgenden Seiten des Assistenten für Formulardefinitionen für Windows-Anwendungen verwendet:

- Formular benennen
- Formular identifizieren
- Sonstige Einstellungen konfigurieren
- Einstellungen bestätigen

Klicken Sie nach Abschluss der Aktionen, die für eine bestimmte Seite erforderlich sind, auf **Weiter**. Die Schaltfläche **Zurück** ist in der Regel auf jeder Seite verfügbar, um zuvor konfigurierte Optionen erneut aufzurufen. Unter Umständen ist es jedoch erforderlich, nachfolgende Einstellungen anzupassen, wenn Sie zuvor konfigurierte Optionen ändern.

Formular benennen

Beim Erstellen von Anwendungsdefinitionen für Webanwendungen wird die Seite **Formular benennen** des Assistenten für Formulardefinitionen für Folgendes verwendet:

- Zuweisen eines benutzerdefinierten Namens für das zu erstellende Formular
- Identifizieren des zu erstellenden Formulartyps
- Identifizieren aller speziellen Aktionen

Bedenken Sie, dass der Name, den Sie dem Formular zuweisen, auf der Seite **Formulare verwalten** des Assistenten für Anwendungsdefinitionen angezeigt wird. Weisen Sie daher einen aussagekräftigen Namen für den zu definierenden Formulartyp zu.

Verschiedene Standardformulartypen zum Verarbeiten von Anmelde-informationen des Benutzers können mit dem Assistenten für Formulardefinitionen definiert werden. Dazu gehören:

- **Anmeldung**

  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.

- **Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Erfolgreiche Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Fehlgeschlagene Kennwortänderung**

  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwort-änderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Verwenden Sie den Bereich **Spezielle Aktionen**, um ggf. spezielle Formularaktionen für das zu definierende Formular zu identifizieren:

- **Keine spezielle Aktion**

  Wählen Sie diese Option für die normale Webformularverarbeitung.

- **Zu Windows-Anwendung umleiten**

  Wählen Sie diese Option aus, wenn im Assistenten für Webformulare kein Formular für die Webanwendung erkannt wurde. (Weitere Informationen finden Sie unter “Formular identifizieren”.) Dies tritt auf, wenn in der Webanwendung ActiveX-Steuerelemente, Flash-basierte Steuerelemente, bestimmte Ajax-Steuerelementtypen oder andere nicht auf HTML basierende Steuerelemente für Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden. Weitere Konfigurationsinformationen finden Sie unter „Zu Windows-Anwendungskonfiguration umleiten“ auf Seite 89.

- **Dieses Formular ignorieren, wenn es von der Agentsoftware erkannt wird**

  Wählen Sie diese Option, damit die Agentsoftware das Formular ignoriert.

Formular identifizieren

Beim Erstellen von Anwendungsdefinitionen für Webanwendungen werden auf der Seite **Formular identifizieren** die Informationen eingegeben, die erforderlich sind, damit das zu definierende Formular von der Password Manager Agent-Software eindeutig erkannt wird.

Webanwendungen werden über die URL-Adresse identifiziert, die dem zu definierenden Formular zum Verwalten von Anmeldeinformationen des Benutzers zugeordnet ist.

Klicken Sie auf **Auswählen**, um den Assistenten für Webformulare zu öffnen. Mit diesem Assistenten werden die URL-Adresse identifiziert und die Aktionen zum Verwalten der Anmeldeinformationen des Benutzers für das zu definierende Formular definiert. (Weitere Informationen finden Sie unter „Assistent für Webformulare“ auf Seite 88).

Nach Abschluss des Assistenten für Webformulare werden Sie zurück auf diese Seite geleitet. Zum Verwalten der Interpretation der identifizierten URLs sind zwei Kontrollkästchen verfügbar:

- Strenge URL-Zuordnung

  Wenn Sie dieses Kontrollkästchen aktivieren, werden Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers nur erkannt, wenn sie von Webanwendungen stammen, die über die angegebenen URLs gestartet wurden. Einige URLs enthalten unter Umständen dynamische Daten wie Kennungen zur Sitzungsverwaltung, Anwendungsparameter oder andere Kennungen, die für jede Instanz unterschiedlich sein können. In diesem Fall wird die URL beim Verwenden der strengen URL-Zuordnung möglicherweise nicht erkannt.

- URL (Groß-/Kleinschreibung)

  Aktivieren Sie dieses Kontrollkästchen, um URLs mit genau übereinstimmender Schreibweise zu verwenden.

Sonstige Einstellungen konfigurieren

Beim Festlegen von Webdefinitionen geben Sie auf dieser Seite an, ob die Agentsoftware automatisch oder der Benutzer manuell auf die Schaltfläche **Senden** klickt.

Aktivieren Sie das Kontrollkästchen **Agent sendet dieses Formular automatisch**, um das Formular automatisch ohne Benutzereingriff zu senden.

Einige Webanwendungen verwenden dynamische URLs. Klicken Sie in diesem Fall auf **Erweitert**, um das Dialogfeld **Erweiterte Einstellungen** aufzurufen, in dem Sie zusätzliche Formulardefinitionskriterien zur Zuordnung des Webformulars festlegen können. (Weitere Informationen finden Sie unter „Dialogfeld „Erweiterte Einstellungen“ für Webanwendungen“ auf Seite 90.)

Einstellungen bestätigen

Die Seite **Einstellungen bestätigen** ist die letzte Seite des Assistenten für Formulardefinitionen. Hier können Sie die Konfigurationsoptionen und Einstellungen überprüfen, die dem Formular zugeordnet wurden. Administratoren können auf dieser Seite die Konfiguration überprüfen, bevor sie das Formular beenden und zum Assistenten für Anwendungsdefinitionen zurückkehren, um weitere Formulare zu definieren bzw. um das Bearbeiten einer Anwendungsdefinition abzuschließen.

Assistent für Webformulare

Mit dem Assistenten für Webformulare wird identifiziert, welche Felder in der ausgewählten Webanwendung Anmeldeinformationen des Benutzers erhalten und welches Steuerelement zum Senden des Formulars verwendet wird.

In der oberen Seitenhälfte wird das identifizierte Formular angezeigt. In der unteren Seitenhälfte werden die identifizierten Formularfelder angezeigt.

Wenn keine Formularfelder identifiziert sind, muss die Formulardefinition zu einer Windows-Anwendung umgeleitet werden, um SendKeys-Optionen zum Verwalten der Formularoberfläche zu verwenden. Stellen Sie in diesem Fall sicher, dass auf der Seite **Formular identifizieren** die Option **Zu Windows-Anwendung umleiten** ausgewählt ist. Weitere Informationen zur Konfiguration finden Sie unter „Zu Windows-Anwendungskonfiguration umleiten“ auf Seite 89.

Klicken Sie sonst mit der rechten Maustaste auf Einträge in der unteren Seitenhälfte, um das entsprechende Formularfeld in der oberen Seitenhälfte zu markieren. Weisen Sie anhand der Markierung die Anmeldeinformationen des Benutzers zu, die in das zugeordnete Feld eingetragen werden sollen. Wiederholen Sie diesen Vorgang für alle Anmeldeinformationen des Benutzers, die dem zu definierenden Formular zum Verwalten von Anmeldeinformationen des Benutzers zugeordnet sind.

Gelegentlich werden Feldnamen dynamisch ausgefüllt. Aktivieren Sie in diesem Fall das Kontrollkästchen **Ordinalzahlen als Feldnamen verwenden**, um die Felder anhand von Ordinalzahlen zu identifizieren. Ordinalzahlen werden selbständig nummeriert und sind unabhängig von Informationen, die von der Anwendung gesendet werden.

Nachdem alle Anmeldeinformationen des Benutzers zugewiesen wurden und Sie das Steuerelement identifiziert haben, das zum Senden des Formulars verwendet werden soll, klicken Sie auf **OK**, um zur Seite „Formular identifizieren“ auf Seite 61 zurückzukehren.

Zu Windows-Anwendungskonfiguration umleiten

Wenn im Assistenten für Webformulare kein Formular für die Webanwendung erkannt wird (siehe „Assistent für Webformulare“ auf Seite 88), muss die Formulardefinition umgeleitet werden, um eine Formulardefinition zu verwenden, die für eine Windows-Anwendung definiert wurde.

Formulare werden unter Umständen nicht erkannt, wenn in der Webanwendung ActiveX-Steuerelemente, Flash-basierte Steuerelemente, bestimmte Ajax-Steuerelementtypen oder andere nicht auf HTML basierende Steuerelemente für Ereignisse zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden.

Stellen Sie in diesen Fällen sicher, dass das Kontrollkästchen **Zu Windows-Anwendung umleiten** auf der Seite **Formular identifizieren** aktiviert ist. (Weitere Informationen finden Sie unter „Formular identifizieren“ auf Seite 61.) Klicken Sie auf **Weiter**, um jede der verbleibenden Seiten des **Assistenten für Formulardefinitionen** zu durchlaufen und klicken Sie auf der Seite **Einstellungen bestätigen** auf **Fertig stellen**.

Die Merkmale der Formularerkennung und Anmeldeinformationsaktionen müssen nun über Windows-Definitionen und SendKeys-Aktionen definiert werden. (Weitere Informationen finden Sie unter „Windows-Anwendungsdefinitionen“ auf Seite 59.)

Dialogfeld „Erweiterte Einstellungen“ für Webanwendungen

Einige Webanwendungen verwenden dynamische URLs. In diesem Fall müssen zusätzliche Formulardefinitionskriterien (so genannte Erkennungszuordnungseinträge) verwendet werden, um ein bestimmtes Formular zum Verwalten von Anmeldeinformationen des Benutzers eindeutig zu identifizieren.

Diese Erkennungszuordnungseinträge werden im Dialogfeld **Zuordnungsdetail** definiert und im Dialogfeld **Erweiterte Einstellungen** angezeigt. Um auf das Dialogfeld **Zuordnungsdetail** zuzugreifen, klicken Sie auf der Seite **Sonstige Einstellungen konfigurieren** auf **Erweitert**. Klicken Sie im dann angezeigten Dialogfeld **Erweiterte Einstellungen** auf **Hinzufügen**.

Definieren Sie mit den Optionen und Steuerelementen im Dialogfeld **Zuordnungsdetail** die Kriterien, die zum eindeutigen Identifizieren eines bestimmten Formulars zum Verwalten von Anmeldeinformationen des Benutzers verwendet werden. Bei dieser Methode wird der mit Tags markierte Inhalt des HTML-Formulars, mit dem eine bestimmte Aktion zum Verwalten von Anmeldeinformationen des Benutzers ausgeführt werden soll, nach bestimmten Werten durchsucht. Sie müssen lediglich so viele Zuordnungsbedingungen definieren, wie für die Identifizierung des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind.

Stellen Sie beim Erstellen eines Erkennungszuordnungseintrags sicher, dass Sie den Quellcode des speziellen HTML-Formulars zum Verwalten von Anmeldeinformationen des Benutzers geöffnet haben, damit Sie Tags und übereinstimmende Kriterien identifizieren können, die dann zum Erstellen von Erkennungszuordnungseinträgen verwendet werden.

1. Klicken Sie auf der Seite **Sonstige Einstellungen konfigurieren** im Assistenten für Formulardefinitionen auf **Erweitert**. Das Dialogfeld **Erweiterte Einstellungen** wird geöffnet.

2. Klicken Sie im Dialogfeld **Erweiterte Einstellungen** auf **Hinzufügen**. Das Dialogfeld **Zuordnungsdetail** wird geöffnet. Erstellen Sie in diesem Dialogfeld einen Erkennungszuordnungseintrag, mit dem das zu definierende Formular eindeutig identifiziert wird. Dieses Dialogfeld ist wie folgt unterteilt:

   - **Tag**

     In diesem Feld suchen Sie das angegebene HTML-Tag. Wenn die bestimmte Instanz des Tags bekannt ist, aktivieren Sie das Kontrollkästchen **Taginstanz zuordnen** und identifizieren Sie die im Dokument zu verwendende Instanz. Wenn keine bestimmte Instanz identifiziert ist, werden alle Instanzen im Dokument ausgewertet. Es muss nur das Tag angegeben werden, nicht das Trennzeichen (z. B. **p** statt <**p**>). Wählen Sie nach Möglichkeit das Tag aus, das dem zuzuordnenden Inhalt am nächsten ist.

     Hinweis: Da die Zuordnungstaginstanzsoption je nach Browser variieren kann, sollten Sie diese Funktion nur bei Bedarf verwenden und die Konfiguration eingehend testen.

   - **Kriterien**

     Definieren Sie in diesem Bereich die Zuordnungskriterien. Wählen Sie eines der folgenden Kriterien aus:

     - Text: Beliebiger Text im HTML-Code.
     - HTML: Beliebiger bestimmter Code im angegebenen Tag
     - Attribut: Beliebiges Attribut des HTML-Codes (z. B. das Attribut **name** des Tags **form**).

- **Wert**

  Geben Sie in dieses Feld den Zuordnungswert ein. Aktivieren Sie das Kontrollkästchen **Ganzen Wert zuordnen**, um eine strenge Wertzuordnung zu erzwingen (jeder nicht angegebene Text im Tagelement lässt die Zuordnung fehlgeschlagen). Geben Sie alle Trennzeichen und Anführungszeichen ein, die auftreten können.

  Hinweis: Das Kontrollkästchen **Ganzen Wert zuordnen** darf nach Möglichkeit nur aktiviert werden, wenn mehrere Instanzen ähnlicher Zuordnungskriterien vorliegen.

- **Operator**

  In diesem Bereich können Sie definieren, in welcher Beziehung dieser Zuordnungseintrag zu anderen Einträgen auf diesem Formular steht. Die folgenden Optionen sind verfügbar:

  - UND: Wählen Sie diese Option aus, wenn nicht nur dieser Zuordnungseintrag, sondern mehrere Zuordnungen erforderlich sind, um das Formular zu identifizieren. Wenn Sie diese Option auswählen, wird das aktuelle Zuordnungsergebnis mit dem nächsten Zuordnungsergebnis verglichen. Wenn beide zutreffen, ist die Zuordnung erfolgreich.
  - ODER: Wählen Sie diese Option aus, wenn diese Zuordnung ausreicht, um das Formular zu identifizieren. Wenn Sie diese Option auswählen, wird das aktuelle Zuordnungsergebnis mit dem nächsten Zuordnungsergebnis verglichen. Wenn eins der beiden zutrifft, ist die Zuordnung erfolgreich. Diese Option wird für Definitionen mit Einzelzuordnung verwendet.
  - NICHT: Verwenden Sie diesen Vorgang, um negative Logik auf den Operator anzuwenden. Dieser Operator wird verwendet, um Zuordnungskriterien zu definieren, die nicht auf der Seite angezeigt werden sollen.

3. Klicken Sie nach dem Erstellen des Erkennungszuordnungseintrags auf **OK**. Danach werden neu erstellte Erkennungszuordnungseinträge im Dialogfeld **Erweiterte Einstellungen** angezeigt.
4. Wiederholen Sie Schritt 2 und 3 für jeden Erkennungszuordnungseintrag, der erforderlich ist, um das zu definierende Formular zum Verwalten von Anmeldeinformationen des Benutzers eindeutig zu identifizieren.
5. Wenn mehrere Erkennungszuordnungseinträge im Dialogfeld **Erweiterte Einstellungen** angezeigt werden, können Sie mit den Schaltflächen **Auf** und **Ab** die richtige Verarbeitungsreihenfolge für die Einträge festlegen. Die Erkennungseinträge werden von oben nach unten ausgewertet und die Auswertungsreihenfolge kann von großer Bedeutung sein, um eine erfolgreiche Zuordnung zu bestätigen.

Host/Mainframe-Anwendungsdefinitionen

Host/Mainframe-Anwendungen dienen zum Identifizieren von hostbasierten Anwendungen, einschließlich Mainframe-, AS/400, OS/390-, UNIX- bzw. anderen hostbasierten Sitzungen. Password Manager bietet Single Sign-On-Funktionalität für hostbasierte Anwendungen durch Terminalemulatoren, die HLLAPI implementieren oder über eine interne Skriptsprache verfügen, mit der ein Dialogfeld angezeigt werden kann.

Erfassen der erforderlichen Informationen für Hostanwendungsdefinitionen

Am besten (und einfachsten) können Sie die für Hostanwendungsdefinitionen erforderlichen Informationen erfassen, indem Sie die Anwendung starten.

Hostbasierte Anwendungsdefinitionen werden mit dem Assistenten für Formulardefinitionen erstellt. Mit dem Assistenten werden eine oder mehrere Textzeichenfolgen identifiziert, die für ein bestimmtes Formular zum Verwalten von Anmeldeinformationen des Benutzers (Benutzeranmeldung, Kennwort ändern, erfolgreiche Kennwortänderung oder fehlgeschlagene Kennwortänderung) auf den Hostanwendungsbildschirmen vorhanden sein müssen (bzw. nicht vorhanden sein dürfen).

Zeichnen Sie beim Aufrufen des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers alle Benutzeraktionen auf, die für den Formularzugriff erforderlich sind. Diese Aktionen sind in der Formulardefinition für jedes Formular erforderlich, wenn der Assistent für Formulardefinitionen über die Konsole bzw. das Anwendungsdefinitionstool ausgeführt wird.

Nach dem Identifizieren des richtigen Formulars zum Verwalten von Anmeldeinformationen des Benutzers werden die Koordinaten der Dateneintragsfelder definiert, die zum Senden der entsprechenden Anmeldeinformationen des Benutzers an die Anwendung verwendet werden. Diese werden durch Festlegen der Aktionsfolge bzw. Tastatureingaben definiert, die zum Wechsel zwischen Feldern oder Bildschildschirmen und zur Texteingabe erforderlich sind.

Der Assistent für Formulardefinitionen wird in folgenden Situationen gestartet:

- Beim Erstellen einer neuen Anwendungsdefinition mit dem Assistenten für Anwendungsdefinitionen
- Beim Bearbeiten eines Formulars in einer vorhandenen Anwendungsdefinition
- Beim Hinzufügen eines Formulars in einer vorhandenen Anwendungsdefinition

Der Anwendungstyp wird identifiziert, wenn eine neue Anwendungsdefinition erstellt wird.

Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53 und „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.

Definieren von Formularen

Bei der Formulardefinition werden die formularspezifischen Identifizierungs- und Aktionsinformationen gesammelt. Dabei werden die folgenden Seiten des Assistenten für Formulardefinitionen für Hostanwendungen verwendet:

- Formular benennen
- Formular identifizieren
- Regeln für Felderkennung einstellen
- Sonstige Einstellungen konfigurieren
- Einstellungen bestätigen

Klicken Sie nach Abschluss der Aktionen, die für eine bestimmte Seite erforderlich sind, auf **Weiter**. Die Schaltfläche **Zurück** ist in der Regel auf jeder Seite verfügbar, um zuvor konfigurierte Optionen erneut aufzurufen. Unter Umständen ist es jedoch erforderlich, nachfolgende Einstellungen anzupassen, wenn Sie zuvor konfigurierte Optionen ändern.

Formular benennen

Beim Erstellen von Anwendungsdefinitionen für Hostanwendungen wird die Seite **Formular benennen** des Assistenten für Formulardefinitionen für Folgendes verwendet:

- Zuweisen eines benutzerdefinierten Namens für das zu erstellende Formular
- Identifizieren des zu erstellenden Formulartyps

Bedenken Sie, dass der Name, den Sie dem Formular zuweisen, auf der Seite **Formulare verwalten** des Assistenten für Anwendungsdefinitionen angezeigt wird. Weisen Sie daher einen aussagekräftigen Namen für den zu definierenden Formulartyp zu.

Verschiedene Standardformulartypen zum Verarbeiten von Anmelde-informationen des Benutzers können mit dem Assistenten für Formulardefinitionen definiert werden. Dazu gehören:

- **Anmeldung**

  Zum Identifizieren der Oberfläche bei der Anmeldung an einer Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für einen Zugriff auf die zugeordnete Anwendung erforderlich sind.

- **Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Erfolgreiche Kennwortänderung**

  Zum Identifizieren der Oberfläche bei der Kennwortänderung für eine Anwendung und zum Verwalten der Aktionen für Anmeldeinformationen des Benutzers, die für ein Ändern des Benutzerkennworts für die zugeordnete Anwendung erforderlich sind.

- **Fehlgeschlagene Kennwortänderung**

  Zum Identifizieren der Oberfläche bei einer fehlgeschlagenen Kennwort-änderung für eine Anwendung und zum Definieren der Aktionen, die bei einer fehlgeschlagenen Änderung der Anmeldeinformationen ausgeführt werden müssen.

In den Versionen 4.0 und 4.1 von Password Manager Agent werden Formulare für die erfolgreiche oder fehlgeschlagene Änderung der Anmeldeinformationen nicht unterstützt und es erfolgt keine Reaktion auf Anwendungsdefinitionen, die diese Formulare enthalten.

Wenn der verwendete Emulator mehr als eine Anmeldungs- oder Kennwortänderungsseite anzeigt, müssen Sie für jede Seite ein Formular erstellen.

Formular identifizieren

Beim Erstellen von Anwendungsdefinitionen für Hostanwendungen werden auf der Seite **Formular identifizieren** die Informationen eingegeben, die erforderlich sind, damit das zu definierende Formular von der Password Manager Agent-Software eindeutig erkannt wird.

Hostanwendungen werden über Textzeichenfolgen identifiziert, die in angegebenen Zeilen- und Spaltenpositionen auf der Hostanwendungsseite angezeigt werden. Es müssen nur so viele Textzeichenfolgezuordnungen definiert werden, wie für eine eindeutige Identifizierung des Hosts erforderlich sind.

So fügen Sie einen qualifizierenden Eintrag für eine Textzuordnung hinzu

1. Stellen Sie sicher, dass die Hostanwendung gestartet wurde und Sie bereits festgelegt haben, welche Textzeichenfolgen zur eindeutigen Identifizierung der Zielanwendung verwendet werden müssen.
2. Klicken Sie auf **Hinzufügen**, um der Liste der Textzuordnungseinträge, die zur Qualifizierung der Anwendung zu verwenden sind, einen neuen Eintrag hinzuzufügen. Das Dialogfeld **Text für Zuordnung** wird geöffnet.

3. Füllen Sie die folgenden Felder im Dialogfeld **Text für Zuordnung** aus:

    - **Textzeichenfolge**

      Geben Sie den genauen Text ein, der zur Identifizierung der Anwendung verwendet werden soll.

    - **Zeile**

      Geben Sie die genaue Zeilennummer für die Zeichenfolge ein.

    - **Spalte**

      Geben Sie die genaue Spaltennummer für die Zeichenfolge ein.

    Hinweis: Wenn die Hostanwendung von der Agentsoftware durchsucht wird, wird im Bildschirm nach der angegebenen Textzeichenfolge in der definierten Zeile und Spalte gesucht. Wenn der Text unter den definierten Koordinaten nicht genau mit dem angegebenen Text übereinstimmt, wird der Bildschirm ignoriert.

    ---

4. Wenn Sie den Zeichenfolgenwert für den Vergleich sowie die Koordinaten, unter denen die Zeichenfolge angezeigt wird, eingegeben haben, klicken Sie auf **OK**. Der definierte Eintrag unter **Text für Zuordnung** wird auf der Seite **Formular identifizieren** angezeigt.
5. Oft müssen zur Identifizierung des fehlerfreien Starts der Ziel-Hostanwendung mehrere Textzeichenfolgen definiert werden. Wiederholen Sie Schritte 2 und 4 für jede Zeichenfolge, wenn mehrere Zeichenfolgen unter **Text für Zuordnung erforderlich** sind.
6. Wenn alle Einträge unter **Text für Zuordnung** definiert wurden, klicken Sie auf **Weiter**, um fortzufahren.

Regeln für die Felderkennung

Auf der Seite **Regeln für Felderkennung einstellen** werden der Speicherort und die Tastenaktionen identifiziert, die zum Verwalten des zu definierenden Formulars für Anmeldeinformationen des Benutzers erforderlich sind.

Dabei sollen Feldeingaben erstellt werden, mit denen festgelegt wird, welche Anmeldeinformationen des Benutzers verarbeitet werden, an welcher Stelle sie auf dem Bildschirm eingefügt werden (Zeilen- und Spaltenkoordinaten) und welche Tastatureingaben zum Bewegen des Mauszeigers zu den nächsten Anmeldeinformationen bzw. zur nächsten Sendeaktion erforderlich sind.

Gehen Sie wie folgt vor, um eine Feldeingabe hinzuzufügen:

1. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Feld definieren** zu öffnen.
2. Füllen Sie die folgenden Felder im Dialogfeld **Feld definieren** aus:
   - **Feldfunktion**

     Wählen Sie im Dropdownlistenfeld die Anmeldeinformationen des Benutzers aus, die gesendet werden sollen.
   - **Zeile**

     Geben Sie die genaue Zeilennummer für die Zeichenfolge ein.
   - **Spalte**

     Geben Sie die genaue Spaltennummer für die Zeichenfolge ein.
   - **Tasten nach**

     Geben Sie die Tastencodes ein, die erforderlich sind, um zum nächsten Anmeldeinformationsfeld zu wechseln oder um eine Sendeaktion auszuführen.

   Hinweis: Wählen Sie den Hyperlink **Virtuelle Tastencodes** aus, um Hilfeinformationen zu gültigen Tastencodes anzuzeigen.
3. Klicken Sie nach der Eingabe aller erforderlichen Daten für die Feldeingabe auf **OK**. Danach wird die definierte Feldeingabe auf der Seite **Regeln für Felderkennung einstellen** angezeigt.

4. Wiederholen Sie die Schritte 1 bis 3 für alle Anmeldeinformationen für Benutzer, die für das Formular definiert werden müssen.
5. Die auf der Seite **Regeln für Felderkennung einstellen** angezeigten Feldeingaben werden entsprechend ihrer Position auf der Seite von oben nach unten verarbeitet. Ordnen Sie die Einträge mit den Pfeiltasten **Auf** und **Ab** in der Reihenfolge an, die für die Verarbeitung des Formulars für Anmeldeinformationen des Benutzers erforderlich ist.
6. Klicken Sie nach der Definition und Anordnung aller Feldeingaben auf **Weiter**.

Sonstige Einstellungen konfigurieren

Die Seite **Sonstige Einstellungen konfigurieren** enthält erweiterte Einstellungsoptionen für das zu definierende Formular. Folgende Optionen sind möglich:

- Definieren einer anfänglichen Verzögerung bei der Formularverarbeitung
- Definieren der erforderlichen Tastatureingaben zum Aufrufen des zu definierenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers
- Definieren, ob EINGABE (nicht ALT-Taste) zum Wechsel zwischen den Formularfeldern verwendet wird
- Definieren der Kriterien für eine Textzeichenfolgenzuordnung zum Ignorieren eines Formulars

Wenn eine zusätzliche erweiterte Konfiguration für das zu definierende Formular zum Verwalten von Anmeldeinformationen des Benutzers erforderlich ist, klicken Sie auf **Erweitert**, um das Dialogfeld **Erweiterte Einstellungen** zu öffnen, und fahren Sie mit „Erweiterte Einstellungen für Hostanwendungen“ auf Seite 101 fort. Klicken Sie andernfalls auf **Weiter**, um fortzufahren.

Einstellungen bestätigen

Die Seite **Einstellungen bestätigen** ist die letzte Seite des Assistenten für Formulardefinitionen. Hier können Sie die Konfigurationsoptionen und Einstellungen überprüfen, die dem Formular zugeordnet wurden. Administratoren können auf dieser Seite die Konfiguration überprüfen, bevor sie das Formular beenden und zum Assistenten für Anwendungsdefinitionen zurückkehren, um weitere Formulare zu definieren bzw. um das Bearbeiten einer Anwendungsdefinition abzuschließen.

Erweiterte Einstellungen für Hostanwendungen

Für einige Hostanwendungen ist eine zusätzliche Konfiguration erforderlich, um sicherzustellen, dass das richtige Formular zum Verwalten von Anmeldeinformationen des Benutzers identifiziert wird. Beispiele:

- Festlegen einer Wartezeit zum Starten der Hostanwendung, bevor versucht wird, die Anwendung zu identifizieren
- Verarbeiten einer Reihe von Tastatureingaben zum Aufrufen der Erstanmeldungs- oder Kennwortänderungsseite
- Ignorieren einer Seite bei der Verarbeitung, wenn bestimmter Text angezeigt wird

Wenn erweiterte Konfigurationseinstellungen für das zu definierende Formular zum Verwalten von Anmeldeinformationen des Benutzers erforderlich sind, klicken Sie auf der Seite **Sonstige Einstellungen konfigurieren** auf **Erweitert**, um das Dialogfeld **Erweiterte Einstellungen** zu öffnen. (Weitere Informationen finden Sie unter „Sonstige Einstellungen konfigurieren" auf Seite 100).

Das Dialogfeld **Erweiterte Einstellungen** enthält zwei Konfigurationsseiten, die über den linken Seitenbereich aufgerufen werden:

- Zusätzliche Einstellungen für Hostformular
- Zuordnung ignorieren

Zusätzliche Einstellungen für Hostformular

Wählen Sie im linken Bereich die Option **Zusätzliche Einstellungen für Hostformular** aus, um auf folgende Optionen für **Zusätzliche Einstellungen** zuzugreifen:

- Feldeingaben verzögern

  Geben Sie die Verzögerung für den Abschluss des Ladevorgangs der Anwendung in Millisekunden ein, bevor das Formular verarbeitet wird.

- Tasten vorher

  Geben Sie die virtuellen Tastencodes ein, mit denen auf das erste Feld des zu verarbeitenden Formulars zum Verwalten von Anmeldeinformationen des Benutzers zugegriffen werden soll. Wählen Sie den Hyperlink **Virtuelle Tastencodes** aus, um die Hilfe für die gültigen Tastencodes anzuzeigen.

- Mit EINGABE- (nicht ALT-Taste) zwischen den Formularfeldern wechseln

  Aktivieren Sie ggf. das Optionsfeld.

Zuordnung ignorieren

Wählen Sie im linken Bereich die Option **Zuordnung ignorieren** aus, um auf die Option **Textzuordnung, die das Senden von Anmeldeinformationen beendet** zuzugreifen. Mit dieser Option können Textzeichenfolgen definiert werden, die auf der Anwendungsseite für Formulare angezeigt werden, die zu ignorieren sind. Die Konfigurationsoptionen sind mit den Optionen unter „Formular identifizieren“ auf Seite 97 identisch.

Überlegungen für Host-Anwendungsdefinitionen

Beachten Sie beim Definieren von Hostanwendungsdefinitionen die folgenden Punkte:

- Für jede Benutzerkonfiguration mit Hostanwendungen muss die Unterstützung von Terminalemulationsprogrammen aktiviert sein.
- Stellen Sie sicher, dass der Terminalemulator HLLAPI-kompatibel ist.
- Stellen Sie sicher, dass der Terminalemulator in der Datei mfrmlist.ini der Agentsoftware definiert ist. (Weitere Informationen finden Sie unter „Unterstützung von Terminalemulationsprogrammen“ auf Seite 103.)
- Sparen Sie Zeit, indem Sie einen Terminalemulator verwenden, in dem die Zeilen- und Spaltenkoordinaten der Mauszeigerposition angezeigt werden. Damit erkennen Sie leichter die Position des Textes und der Felder für die Identifizierung der Hostanwendung und der zugehörigen Anmeldeformulare.
- Für die HLLAPI-Erkennung muss der Terminalemulator für jede Sitzung einen Kurznamen festlegen. Die Agentsoftware kann eine hostbasierte Anwendung nicht ohne den Kurznamen der Terminalemulatorsitzung erkennen.
- Die Dokumentation für die hostbasierte Anwendung enthält unter Umständen eindeutige Kennungen (z. B. Bildschirmnummern) für die Bildschirme, die zum Senden der Anmeldeinformationen des Benutzers verwendet werden. Verwenden Sie in diesem Fall die Bildschirmnummer als eindeutige Kennung, um sicherzustellen, dass die Anmelde-informationen für das richtige Formular von der Agentsoftware identifiziert und gesendet werden.

Unterstützung von Terminalemulationsprogrammen

Die unterstützten Terminalemulatoren sind in der Datei Mfrmlist.ini enthalten. Diese Datei umfasst alle Terminalemulatoren, die von Citrix getestet wurden.

Die Liste kann um weitere Emulatoren erweitert werden. Neue Definitionen sollten jedoch getestet und geprüft werden, bevor Sie sie in Ihre Produktionsumgebung integrieren. Im Folgenden finden Sie einen Beispielabschnitt dieser Datei:

```
[Emulators]
Ver=20021101
EMU1=Rumba6
EMU2=Attachmate myExtra!
EMU3=Attachmate Extra! 6.3
EMU4=Attachmate Extra! 6.4
EMU5=Attachmate Extra! 6.5
EMU6=Attachmate Extra! 2000
EMU7=Attachmate Extra! 7.1
EMU8=Reflection7
EMU9=Reflection8
EMU10=Reflection9
EMU11=Reflection10
EMU12=PCOM
EMU13=HostOnDemand 4.1
EMU14=GLink
EMU15=Aviva
EMU16=ViewNow
EMU17=ZephyrPC
EMU18=ZephyrWeb
;EMU19=BOSaNOVA
;EMU20=HostExplorer6
;EMU21=HostExplorer8
[Rumba6]
DisplayName=Rumba
RegistryLoc=WALLDATA\Install
ValueName=
```

```
DLLFile=SYSTEM\EHLAPI32.DLL
UpdateNotificationHandling=0.FirstLogin
Process=shared
ConvertPosType=long
QuerySessionsType=long
QuerySessionStatusType=long
QueryHostUpdateType=long
StartNotificationType=long
IntSize=16
WindowClass=WdPageFrame
WindowTitle=RUMBA
```

Die Emulatoreinträge im Abschnitt **[Emulators]** der Datei Mfrmlist.ini müssen numerisch geordnet sein – von „EMU1" bis „EMU99". Jede Unterbrechung der Reihenfolge führt dazu, dass der Prozess Ssomho.exe beendet wird, bevor alle Einträge gelesen wurden.

Durch Entfernen oder Auskommentieren nicht verwendeter Emulatoren kann der Startprozess verbessert werden, weil Ssomho.exe dann keine Ressourcen oder Zeit mit der Suche nach dem Speicherort nicht benötigter HLLAPI-DLLs verschwendet.

Zum Auskommentieren eines Eintrages verschieben Sie den entsprechenden Eintrag an das Ende der Liste, setzen Sie vor den Eintrag ein Semikolon und nummerieren Sie dann die restlichen EMU-Einträge neu, sodass kein Nummerierungswert ausgelassen wird.

Password Manager kann die Datei mfrmlist.ini nicht global aktualisieren. Sie müssen die Datei daher nach dem Installieren der Agentsoftware manuell überschreiben. Bei großen Bereitstellungen empfiehlt Citrix die Verwendung von Batchdateien oder Skripten, die über eine System Management Server (SMS)-, CA-Unicenter- oder Active Directory-Softwareinstallation ausgeführt werden.

Felddefinitionen in Mfrmlist.ini

Emulatoren, die der Datei Mfrmlist.ini hinzugefügt wurden, funktionieren nur, wenn sie dem HLLAPI-Standard entsprechen. Die Felddefinitionen für die Datei Mfrmlist.ini können Sie der Tabelle unten entnehmen. Wenn Sie eine Emulatordefinition hinzufügen müssen, erkundigen Sie sich beim Hersteller des Emulators, ob der Emulator HLLAPI unterstützt, und besorgen Sie sich dort die richtigen Felddefinitionseinträge. Um festzustellen, ob ein Emulator mit Password Manager funktioniert, testen Sie ihn außerhalb der Produktionsumgebung.

Feld	Definitionen
[EmulatorName]	Der Wert für **EmulatorName** muss mit dem Wert der Zeile **EMUnn=EmulatorName** im Abschnitt **[Emulators]** übereinstimmen.
GroupName	Nur für den internen Gebrauch.
DisplayName	Anzeigename des Emulators. Einer von zwei Parametern, der verwendet wird, wenn ein neuer Prozess für die Sitzung initiiert wird. Muss innerhalb der Datei Mfrmlist.ini eindeutig sein.
RegistryLoc	Registrierungsschlüssel in HKEY_LOCAL_MACHINE\SOFTWARE, der auf den Pfad verweist, in dem die HLLAPI-DLL gespeichert ist. Wenn das Programm diese Information nicht unter HKEY_LOCAL_MACHINE\SOFTWARE speichert, verwenden Sie statt der Einstellung **RegistryLoc** die Einstellung **ExplicitPath**. Wenn sowohl die Einstellung **RegistryLoc** als auch die Einstellung **ExplicitPath** definiert wurde, hat die Einstellung **ExplicitPath** Vorrang.
ExplicitPath	Expliziter Pfad zu der HLLAPI-DLL-Datei, die dieser Emulator verwendet. Diese Einstellung wird anstelle der Einstellung **RegistryLoc** verwendet, wenn das Emulatorprogramm den Speicherort der HLLAPI-DLL nicht in der Systemregistrierung speichert. Wenn sowohl die Einstellung **RegistryLoc** als auch die Einstellung **ExplicitPath** definiert wurde, hat die Einstellung **ExplicitPath** Vorrang.
ValueName	Name des Wertes im Schlüssel **RegistryLoc**, der den tatsächlichen Pfadwert enthält.
DLLFile	Name der HLLAPI-DLL-Datei.
StripFileName	Gibt an, dass der in ValueName gespeicherte Wert einen umgekehrten Schrägstrich (\) enthält, der beim Zusammenstellen des HLLAPI-DLL-Pfades aus den Einträgen ValueName und DLLFile entfernt werden muss.
IntSize	Definiert die vom Emulator unterstützte Ganzzahlgröße (16 Bit oder 32 Bit).

Feld	Definitionen
WindowClass	Fensterklassenname für den Emulator. Wird mit der Password Manager Console bzw. dem Anwendungsdefinitionstool abgerufen.
WindowTitle	Teil des Fenstertitels, mit dem Password Manager feststellen kann, dass dieses Fenster mit dem Emulator verknüpft ist. Muss mindestens ein Wort enthalten. Dieses wird immer im Fenstertitel angezeigt. Auf beiden Seiten des Textes werden Platzhalterzeichen angenommen.
UseSendKeys	Weist Password Manager an, für die Kommunikation mit dem Emulator SendKeys zu verwenden. Die Option ist nicht mit der für Windows-Anwendungen verwendeten Option identisch.

Weitere Informationen zu Terminalemulatoren finden Sie unter „Vorgänge“ auf Seite 243.

- „Unterstützen von Terminalemulatoren“ auf Seite 255
- „Terminalemulator-basierte Anwendungen“ auf Seite 253

Erstellen von Benutzerkonfigurationen

Hinweis: Wenn Sie als zentralen Speicher einen freigegebenen Novell Ordner verwenden, können Sie nur eine Benutzerkonfiguration erstellen. Citrix Password Manager unterstützt in dieser Situation keine hierarchischen Konfigurationen oder Konfigurationen auf Benutzerebene.

Mit Benutzerkonfigurationen können Sie das Verhalten und die Darstellung der Agentsoftware für Benutzer steuern. Das Erstellen einer oder mehrerer Benutzerkonfigurationen ist der letzte Schritt, den Sie ausführen müssen, bevor Sie Citrix Password Manager Agent an die Benutzer in der Umgebung verteilen. Es können jedoch auch nachträglich noch jederzeit Benutzerkonfigurationen hinzugefügt oder bearbeitet werden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen“ auf Seite 144
- „Zuweisen von Prioritäten zu Benutzerkonfigurationen“ auf Seite 146
- „Zuweisen einer Benutzerkonfiguration zu verschiedenen Benutzern“ auf Seite 147
- „Aktualisieren vorhandener Benutzerkonfigurationen“ auf Seite 149

Hinweis: Weitere Informationen finden Sie unter „Planen der Password Manager-Umgebung“ im *Citrix Password Manager-Installationshandbuch*.

Merkmale von Benutzerkonfigurationen

Eine Benutzerkonfiguration ist eine eindeutige Zusammenstellung von Einstellungen, Kennwortrichtlinien und Anwendungen, die Sie auf Benutzer anwenden, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind.

Eine Benutzerkonfiguration beinhaltet Folgendes:

- Benutzer, die Active Directory-Hierarchien (Organisationseinheiten [OU] oder Einzelbenutzer) oder Active Directory-Gruppen zugeordnet sind

  Hinweis: Verteilergruppen und lokale Gruppen der Domänen im gemischten Modus von Active Directory werden nicht unterstützt.

- Lizenztyp und für die Benutzer geltende Einstellungen (Lizenzierungsmodell: Gleichzeitige oder benannte Benutzer)
- Datenschutzmethoden (siehe „Verwenden der Identitätsprüfung“ und „Planen der Benutzerkonfigurationen“ im *Citrix Password Manager-Installationshandbuch*)
- Erstellte Anwendungsdefinitionen, die Sie bei der Erstellung einer Benutzerkonfiguration in einer Anwendungsgruppe zusammenfassen können
- Kennwortrichtlinien, die für bestimmte Anwendungsgruppen gelten
- Konto-Self-Service-Funktionen (Aufhebung der Kontosperrung und Kennwortzurücksetzung) und Schlüsselverwaltungsoptionen (Verwendung von alten Kennwörtern, Sicherheitsfragen und automatische Schlüsselverwaltung)
- Einstellungen für Optionen wie z. B. Provisioning von Anmeldeinformationen und Anwendungssupport

Standardeigenschaften von Benutzerkonfigurationen

In der folgenden Tabelle werden die Eigenschaften von Benutzerkonfigurationen aufgeführt. Sie können hier Ihre eigenen Einstellungen eintragen.

Eigenschaft der Benutzerkonfiguration	Standard-einstellung	Benutzer-definierte Einstellung
Kontozuordnung		
Standarddomäne für die Kontozuordnung	Nicht eingegeben	
Standarddienstadresse für die Kontozuordnung	Nicht eingegeben	
Benutzerseitiges Zuordnen der Konten	Nein	
Benutzerseitiges Bearbeiten der Domäne	Nein	
Benutzerseitiges Bearbeiten der Dienstadresse	Nein	
Benutzer können Kennwort speichern	Nein	
Agentbenutzeroberfläche		
Computername in QuickInfo des Infobereichssymbols anzeigen	Nein	
Im Anmeldungsmanager standardmäßig angezeigte Spalten und -reihenfolge festlegen	Anwendungs-name, Beschreibung, Gruppe, Zuletzt ver-wendet, Kenn-wort, URL Modul, Benutzername/ ID	
Symbol im Infobereich anzeigen	Ja	
Verzögerung für das agentseitige Senden der Anmeldeinformationen angeben	0 Sekunden	
Anwendungsunterstützung		
Clientseitige Anwendungsdefinitionen erkennen	Alle Anwen-dungen	
Support für Terminalemulatoren aktivieren	Nein	
Anzahl der Domänennamenstufen für Zuordnung	99	
Zeitintervall, in dem der Agent prüft, ob Terminalemulatoränderungen aufgetreten sind	3000 Millise-kunden	

Eigenschaft der Benutzerkonfiguration	Standard-einstellung	Benutzer-definierte Einstellung
Grundlegendes Agentverhalten		
Benutzerseitiges Anhalten der Agentsoftware	Ja	
Benutzerseitiges Anzeigen aller Kennwörter im Anmeldungsmanager	Nein	
Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern	Ja	
Definierte Formulare automatisch verarbeiten, wenn sie von der Agentsoftware erkannt werden	Ja	
Neuauthentifizierung vor dem Anzeigen der Benutzerkennwörter erzwingen	Ja	
Benutzer über Fehlschlagen der Agentsynchronisierung benachrichtigen	Ja	
Zeitraum zwischen Agent-Anfragen für die Neuauthentifizierung	8 Stunden	
Clientseitiges Verhalten		
Datenordner und Registrierungsschlüssel des Benutzers beim Beenden der Agentsoftware löschen	Nein	
Benutzer können die Speicherung der Anmelde-informationen abbrechen, wenn eine neue Anwendung festgestellt wird	Ja	
Kennwortzuordnung bei der Ersteinrichtung der Anmeldeinformationen erzwingen	Ja	
Anzahl der Tage einschränken, für die gelöschte Anmeldeinformationen verfolgt werden	180 Tage	
Citrix Password Manager-Ereignisse mit der Windows-Ereignisprotokollierung aufzeichnen	Nein	
Datenschutzmethoden		
Schutz mit leeren Kennwörtern zulassen	Nein	
Smartcard-PINs zulassen	Nein	
Microsoft Data Protection API	Nein	
Administratorkontozugriff auf Benutzerdaten steuern	Ja	
Smartcardzertifikat	Nein	
Smartcardschlüsselquelle	Smartcard-Datenschutz	
Authentifizierungsdaten der Benutzer	Ja	

Eigenschaft der Benutzerkonfiguration	Standard-einstellung	Benutzer-definierte Einstellung
Hotdesktop		
Grafik aktivieren	Nein	
Sitzungsanzeige aktivieren	Ja	
Grafikpfad		
Sperrtimeout	Alle 10 Minuten	
Skriptpfad für Sitzungseinstellungen		
Sitzungstimeout	Alle 5 Minuten	
Schlüsselverwaltungsmodul		
Dienstspeicherort		
Lizenzierung		
Lizenzverbrauch für Offlineverwendung zulassen	Nein	
Zeitraum für getrennten Modus für gleichzeitige Benutzer	1 Stunde 30 Minuten	
Fortfahren ohne Prüfung der Lizenzierungsinformationen	Nein	
Name und Portnummer des Lizenzservers	Server:Port	
Zeitraum für getrennten Modus für benannten Benutzer	21 Tage	
Produktedition		
Produktedition	Produktedition auswählen	
Provisioningmodul		
Provisioning verwenden	Nein	
Speicherort für Provisioningdienst		
Sekundäre Datenschutzmethode		
Methode zur Identitätsprüfung	Altes Kenn-wort	
Self-Service-Funktionen		
Zurücksetzen des Domänenkennworts	Nein	
Aufheben der Sperrung des Domänenkontos	Nein	
Synchronisierung		

Eigenschaft der Benutzerkonfiguration	Standard-einstellung	Benutzer-definierte Einstellung
Agentausführung ohne Wiederverbindung zum zentralen Speicher zulassen	Ja	
Benutzerseitiges Aktualisieren der Agenteinstellungen	Ja	
Zugriff auf Anmeldeinfo über das Modul 'Synchronisierung der Anmeldeinformationen' zulassen	Nein	
Immer synchronisieren, wenn Benutzer erkannte Anwendungen oder den Anmeldungsmanager starten	Nein	
Zeitraum zwischen automatischen Synchronisierungsanfragen	Alle 0 Minuten	

Einführung

Hinweis: Weitere Informationen finden Sie unter „Kontoanforderungen zum Installieren und Verwenden von Password Manager“ im *Citrix Password Manager-Installationshandbuch*.

- Vor dem Erstellen von Benutzerkonfigurationen müssen Sie Folgendes erstellt bzw. definiert haben:
  - Zentraler Speicher
  - Anwendungsdefinitionen
  - Kennwortrichtlinien
  - Sicherheitsfragen
- Sie müssen die Benutzerkonfigurationen erstellen, bevor Sie Password Manager Agent für die Benutzer bereitstellen. Unter anderem werden in einer Benutzerkonfiguration der Lizenzserver und die Lizenzierungs-informationen festgelegt, die die Agentsoftware für den Betrieb benötigt.

Im folgenden Abschnitt werden die Punkte beschrieben, die Sie beachten müssen, bevor Sie Benutzerkonfigurationen erstellen:

Angeben der Domänencontroller für Benutzerkonfigurationen

In Umgebungen mit einem Active Directory-basierten zentralen Speicher und mehreren Domänencontrollern können Sie auswählen, an welchen Domänencontroller eine Benutzerkonfiguration beim Schreiben in den zentralen Speicher gebunden werden.

Durch diese Bindung werden die durch die Active Directory-Replikation verursachten Synchronisierungsverzögerungen verringert. Diese Verzögerungen können auftreten, wenn Benutzer gleichzeitig an mehreren Active Directory-Standorten auf Password Manager zugreifen.

Bei der Discovery, die über die Konsole gestartet wird, ermittelt Password Manager alle Domänencontroller in der Domäne. Anschließend können Sie die erstellten Benutzerkonfigurationen an bestimmte Domänencontroller binden, indem Sie den jeweiligen Controller bei der Erstellung der Benutzerkonfiguration auswählen.

So können Sie zum Beispiel festlegen, dass die Benutzer im lokalen Netzwerk an einen Domänencontroller gebunden werden. Nach der Angabe eines Domänencontrollers binden sich Benutzer bei der nächsten Anmeldung an Password Manager an diesen Domänencontroller.

In der Standardeinstellung binden sich Benutzer an jeden nicht schreibgeschützten Domänencontroller, wenn Sie nicht einen Domänencontroller festlegen. Sie können die Einstellung für den Domänencontroller jederzeit ändern, ohne die Integrität der Benutzerdaten zu gefährden, indem Sie die Benutzerkonfiguration ändern.

Hinweis: Stellen Sie bei der Auswahl eines Domänencontrollers sicher, dass die verfügbaren Ressourcen auf dem Domänencontroller den Datenverkehr handhaben können, den Benutzer generieren, wenn sie zu Stoßzeiten eine Verbindung mit dem Domänencontroller herstellen.

Wenn der angegebene Domänencontroller nicht verfügbar oder offline ist, verwendet die Agentsoftware die Benutzerdaten aus dem lokalen Speicher (d. h. die Benutzerdaten auf dem PC des Benutzers). Wenn der Domänencontroller über einen bestimmten (von Ihnen festgelegten) Zeitraum offline ist, können Sie in der Konsole den Task **Benutzerkonfiguration bearbeiten** starten und einen anderen Domänencontroller auswählen oder die Option **Jeder nicht schreibgeschützte Domänencontroller** aktivieren.

So legen Sie einen Domänencontroller für eine bestehende Benutzerkonfiguration fest

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie eine Benutzerkonfiguration aus.
4. Klicken Sie unter **Häufige Tasks** auf **Benutzerkonfiguration bearbeiten**.
5. Der Assistent **Benutzerkonfiguration bearbeiten** wird angezeigt. Wählen Sie links auf der Seite des Assistenten aus den Optionen **Synchronisierungsserver angeben** aus.
6. Wählen Sie einen verfügbaren Domänencontroller oder wählen Sie **Jeder nicht schreibgeschützte Domänencontroller**.
7. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Je nach der von Ihnen ausgewählten Einstellung binden sich die Benutzer, die zur angegebenen Benutzerkonfiguration gehören, bei der nächsten Anmeldung an Password Manager an den festgelegten oder nicht schreibgeschützten Domänencontroller.

Erstellen von Benutzerkonfigurationen: Assistent für Benutzerkonfigurationen

Mit dem Assistenten für Benutzerkonfigurationen können Sie das Verhalten der Agentsoftware mit Password Manager steuern, und welche Funktionen in der Umgebung verwendet werden.

Der Assistent besteht aus den folgenden Seiten:

- „Benennen von Benutzerkonfigurationen“ auf Seite 117
- „Auswählen der Produktedition“ auf Seite 117
- „Auswählen der Anwendungen“ auf Seite 118
- „Agentverhalten konfigurieren“ auf Seite 120
- „Lizenzierung konfigurieren“ auf Seite 127
- „Datenschutzmethoden auswählen“ auf Seite 129
- „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132
- „Self-Service-Funktionen aktivieren“ auf Seite 133
- „Dienstmodule suchen“ auf Seite 133
- „Beenden des Assistenten für Benutzerkonfigurationen“ auf Seite 134

So erstellen Sie eine Benutzerkonfiguration

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Klicken Sie unter **Häufige Tasks** auf **Benutzerkonfiguration hinzufügen**.

Benennen von Benutzerkonfigurationen

- **Benennen der Benutzerkonfiguration**

  Sie sollten die Benutzerkonfigurationen nach der geplanten Gruppierung der Benutzer und Zuweisung von Anwendungen benennen. Beispiel: Benutzer Marketing, Benutzer Softwareentwicklung, Benutzer Nordamerika usw.

- **Zuordnen der Benutzerkonfiguration**

  Es stehen zwei Möglichkeiten zur Auswahl: Benutzer können einer Active Directory-Hierarchie (OU oder Einzelbenutzer) oder einer Active Directory-Gruppe zugeordnet werden. Bei Bedarf können Sie die Benutzerkonfiguration später einer anderen Hierarchie oder Gruppe zuordnen, indem Sie unter **Häufige Tasks** auf **Benutzerkonfiguration verschieben** klicken.

Hinweis: Die Organisation der Active Directory-Umgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Wenn Sie sowohl Active Directory-Hierarchien als auch Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer *gemischten Umgebung*.

Wenn ein Benutzer zu zwei verschiedenen Active Directory-Gruppen gehört und jede der Gruppen einer Benutzerkonfiguration zugeordnet ist, hat die Benutzerkonfiguration mit der höchsten Priorität Vorrang und wird verwendet.

Das Zuordnen von Benutzerkonfigurationen zu Gruppen wird nur in Active Directory-Domänen unterstützt, die die Active Directory-Authentifizierung verwenden.

Auswählen der Produktedition

Wählen Sie die Password Manager-Produktedition aus, die dieser Benutzerkonfiguration zugeordnet wird: Presentation Server Platinum, Password Manager Enterprise oder Password Manager Advanced.

Hinweis: Die Funktionalität und die Verwaltung der Presentation Server Platinum und Password Manager Enterprise Editionen ist identisch. Wenn Sie Citrix Presentation Server 4.5 mit Feature Pack 1, Platinum Edition, verwenden, wählen Sie **Presentation Server Platinum** aus der Liste aus.

Synchronisierungsserver angeben

Wenn Sie Active Directory verwenden, wählen Sie einen verfügbaren Domänencontroller oder **Jeder nicht schreibgeschützte Domänencontroller** aus. Weitere Informationen finden Sie unter „Angeben der Domänencontroller für Benutzerkonfigurationen“ auf Seite 114.

Auswählen der Anwendungen

Fügen Sie die Anwendungen für die Benutzerkonfiguration hinzu. Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird ein Dialogfeld mit den von Ihnen erstellten Anwendungsdefinitionen angezeigt. Diese können Sie hinzufügen, um eine Anwendungsgruppe zu erstellen.

- **Benennen der Anwendungsgruppe**

  Sie sollten die Anwendungsgruppe nach der geplanten Gruppierung der Anwendungen benennen. Beispiel: Webanwendungen, Citrix Software usw. Eine Gruppe kann auch nur eine Anwendung enthalten.

- **Auswählen der Kennwortrichtlinie**

  Wählen Sie die **Standardrichtlinie**, **Domänenrichtlinie** oder eine benutzerdefinierte Kennwortrichtlinie aus, die auf alle Anwendungen in der Gruppe angewendet wird.

- **Diese Anwendungsgruppe zu einer Kennwortgruppe machen**

  Sie können eine Kennwortgruppe erstellen und so die Kennwortänderung automatisieren und vereinfachen. Wenn das Kennwort für eine zu einer Kennwortgruppe gehörenden Anwendungsdefinition geändert wird, stellt die Agentsoftware sicher, dass die Kennwortänderung in den gespeicherten Anmeldeinformationen aller Anwendungen in der Gruppe umgesetzt wird.

Durch die Verwendung von Kennwortgruppen kann die Agentsoftware mehrere Anmeldeinformationen für Anwendungen verwalten, die dieselbe Authentifizierungsstelle verwenden. Wenn Sie zwei Anwendungen haben, beispielsweise eine Finanzanwendung und eine Personalanwendung, die zum Authentifizieren dieselbe Oracle-Datenbank verwenden, können Sie diese beiden Anwendungen in dieselbe Kennwortgruppe einordnen. Sobald ein Benutzer sein Kennwort für eine der Anwendungen ändert, werden die Anmeldeinformationen in der anderen Anwendung automatisch aktualisiert.

Wichtig: Stellen Sie sicher, dass alle Kennwörter in der Kennwortgruppe von derselben Authentifizierungsstelle verwaltet werden. Das Implementieren einer Kennwortgruppe ist zum Beispiel dann sinnvoll, wenn die Anwendungen in einer Kennwortgruppe dieselbe Back-End-Authentifizierungsstelle (wie z. B. eine Datenbank) verwenden, und der Benutzer für jede Anwendung die gleichen Anmeldeinformationen eingeben würde, um sich an der Datenbank zu authentifizieren. Nicht in Zusammenhang stehende Anwendungen (z. B. ein E-Mail-Programm, eine Webanwendung und ein benutzerdefiniertes Programm im Intranet, für das Single Sign-On aktiviert ist), für die ein Benutzer potenziell jeweils verschiedene Anmeldeinformationen eingeben könnte und nur durch Zufall dieselben, würden nicht in einer Gruppe zusammengefasst werden. Wenn ein Benutzer in einem solchen Fall seine Anmeldeinformationen für eine Anwendung in dieser Kennwortgruppe ändert, folgt daraus nicht zwingend, dass diese Anmeldeinformationen auch für die anderen beiden Anwendungen gültig sind.

- **Aktivieren der Ersteinrichtung der Anmeldeinfo**

  Aktivieren Sie diese Option, um den Benutzern zu erlauben, bei der ersten Verwendung von Password Manager Agent (d. h. während der Registrierung) Anmeldeinformationen für die Anwendung festzulegen. Mit dieser Funktion verringern Sie den Aufwand für die Benutzer, da sie die Anmeldeinformationen für die Anwendungen sofort konfigurieren können.

  Aktivieren Sie diese Funktion nicht, wenn die Benutzer die Anmeldeinformationen für jede Anwendung einzeln eingeben, wenn die Anwendung gestartet wird.

Hinweis: Wenn Sie dieser Benutzerkonfiguration später zusätzliche Anwendungen hinzufügen und diese Option aktiviert ist, werden die Benutzer aufgefordert, die Anmeldeinformationen beim nächsten Start der Agentsoftware auf der Arbeitsstation oder dem Clientgerät zu speichern.

Agentverhalten konfigurieren

Auf dieser Seite können Sie das Verhalten der Agentsoftware für alle Benutzer in der Umgebung festlegen. Unter „Erweiterte Einstellungen“ auf Seite 122 werden die erweiterten Agenteinstellungen beschrieben.

- **Benutzerseitiges Anzeigen aller Kennwörter im Anmeldungsmanager**

  Aktivieren Sie diese Option, wenn den Benutzern die den Anwendungen zugeordneten Kennwörter in der Benutzerkonfiguration angezeigt werden.

  Hinweis: Damit die Benutzer ihre Anwendungskennwörter einsehen können, müssen Sie außerdem die Option zum Anzeigen von Kennwörtern in der Kennwortrichtlinie aktivieren, die Sie auf der Seite **Anwendungen auswählen** ausgewählt haben.

- **Neuauthentifizierung vor dem Anzeigen der Benutzerkennwörter erzwingen**

  Aktivieren Sie diese Option, um die Benutzer zu zwingen, zuerst ihre Windows-Anmeldeinformationen einzugeben, bevor sie ihre Kennwörter einsehen können. Diese Option ist standardmäßig aktiviert. Sie können diese Option aktivieren oder deaktivieren, wenn Sie die Option **Benutzerseitiges Anzeigen aller Kennwörter im Anmeldungsmanager** aktiviert haben.

- **Benutzerseitiges Anhalten der Agentsoftware**

  Wenn Sie diese Option aktivieren, können die Benutzer verhindern, dass die Agentsoftware Anmeldeinformationen an Anwendungen sendet. In diesem Fall setzt die Agentsoftware die Erkennung und Beantwortung von Anwendungen vorübergehend aus und die Benutzer müssen ihre Anmeldeinformationen manuell eingeben. Der Agent wird angehalten, aber nicht beendet.

- **Benutzer über Fehlschlagen der Agentsynchronisierung benachrichtigen**

  Aktivieren Sie diese Option, wenn die Benutzer benachrichtigt werden sollen, wenn die Agentsynchronisierung fehlschlägt. Abhängig von der Einstellung **Agentausführung ohne Wiederverbindung zum zentralen Speicher zulassen** auf der Seite **Erweiterte Agenteinstellungen** unter **Synchronisierung** können Benutzer nach dem Fehlschlagen der Synchronisierung ggf. weiterarbeiten.

- **Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern**

  Aktivieren Sie diese Option, wenn die Benutzer aufgefordert werden sollen, für Anwendungen, die von der Agentsoftware neu erkannt wurden, ihre Anmeldeinformationen in Passwort Manager einzugeben.

  Deaktivieren Sie diese Option, wenn Password Manager Agent keine Anwendungen erkennen soll, die nicht dieser Benutzerkonfiguration zugeordnet sind. Wenn diese Option deaktiviert ist, müssen die Benutzer ihre Anmeldeinformationen für diese Anwendungen manuell eingeben. Verwenden Sie diese Einstellung, um zu verhindern, dass Benutzer Anwendungen, die aktuell nicht zu ihrer zugewiesenen Benutzerkonfiguration gehören, den Single Sign-On-Anwendungen hinzufügen.

  Wenn diese Option deaktiviert ist, wird die Option **Benutzer können die Speicherung der Anmeldeinformationen abbrechen, wenn eine neue Anwendung festgestellt wird** auf der Seite **Clientseitiges Verhalten** außer Kraft gesetzt. Falls Sie planen, Provisioning zu verwenden, wird durch das Deaktivieren dieser Option auch verhindert, dass die Benutzer aufgefordert werden, ihre Anmeldeinformationen einzugeben. Unter „Automatisieren der Eingabe der Anmeldeinformationen mit dem Provisioning“ auf Seite 189 wird das Provisioning-Dienstmodul beschrieben.

- **Definierte Formulare automatisch verarbeiten, wenn sie von der Agentsoftware erkannt werden**

  Aktivieren Sie diese Option, damit die Agentsoftware gespeicherte Anmeldeinformationen automatisch ohne Eingriff des Benutzers senden darf. Wenn Sie die dazugehörige Option **Agent sendet dieses Formular automatisch** in der dieser Benutzerkonfiguration zugeordneten Anwendungsdefinition aktiviert haben, werden die Felder zur Eingabe der Anmeldeinformationen in der Anwendung automatisch ausgefüllt.

- **Zeitraum zwischen Agent-Anfragen für die Neuauthentifizierung**

  Geben Sie den Zeitraum zwischen Agentanfragen zur Neuauthentifizierung an. Wenn dieser Zeitraum abläuft, wird der PC des Benutzers gesperrt und der Benutzer muss sich neu authentifizieren, indem er seine Windows-Anmeldeinformationen eingibt. Der Mindestwert für diese Einstellung ist eine Minute.

Erweiterte Einstellungen

Klicken Sie auf der Seite **Agentverhalten konfigurieren** auf die Schaltfläche **Erweiterte Einstellungen**, um auf diese Einstellungen zuzugreifen.

Agentbenutzeroberfläche	
Computername in QuickInfo des Infobereichssymbols anzeigen	Steuert, ob der Computername im QuickInfo des Infobereichssymbols angezeigt wird (im Infobereich der Taskleiste des Benutzers). Wenn die Option aktiviert ist, wird der Computername dem QuickInfo des Symbols im Infobereich angehängt. Diese Option ist in Citrix Presentation Server-Umgebungen und in gemischten Umgebungen (mit veröffentlichten und lokalen Anwendungen) hilfreich, damit die Benutzer sehen können, welcher Agent ausgeführt wird.
Symbol im Infobereich anzeigen	Diese Option ist standardmäßig aktiviert. Sie steuert, ob das Citrix Password Manager Symbol im Infobereich angezeigt wird, wenn der Agent aktiv ist. Wenn das Symbol deaktiviert ist, können die Benutzer die Agentsoftware nicht starten oder beenden oder auf andere benutzergesteuerte Optionen zugreifen.
Verzögerung für das agentseitige Senden der Anmeldeinformationen angeben	Gibt an, wie lange (in Sekunden) der Agent nach dem Erkennen einer zulässigen Anwendung das Senden der Anmeldeinformationen verzögert. Stellen Sie mit dieser Einstellung sicher, dass die Anwendung zum Empfang der Anmeldeinformationen bereit ist. In diesem Zeitraum zeigt die Agentsoftware ein animiertes Symbol an, das angibt, dass der Agent einen Vorgang ausführt.
Im Anmeldungsmanager standardmäßig angezeigte Spalten und -reihenfolge festlegen	Steuert, welche Spalten und in welcher Reihenfolge die Spalten in der Detailansicht des Anmeldungsmanagers angezeigt werden. Diese Einstellung hat keine Auswirkung auf die Ansichten **Liste** oder **Symbol** im Anmeldungsmanager.
Clientseitiges Verhalten	
Kennwortzuordnung bei der Ersteinrichtung der Anmeldeinformationen erzwingen	Diese Option ist standardmäßig aktiviert. Steuert, ob Benutzer bei der Ersteinrichtung der Anmeldeinformationen die Kennwörter zur Bestätigung zweimal eingeben müssen.
Citrix Password Manager-Ereignisse mit der Windows-Ereignisprotokollierung aufzeichnen	Steuert, ob Fehler- und Warnereignisse der Agentsoftware im Windows-Ereignisprotokoll der lokalen Arbeitsstation aufgezeichnet werden.

Datenordner und Registrierungsschlüssel des Benutzers beim Beenden des Agents löschen	Steuert, ob die Registrierungsschlüssel und Datenordner des Benutzers, einschließlich der verschlüsselten Anmeldeinformationen, gelöscht werden, wenn der Agent beendet wird.
Benutzer können die Speicherung der Anmeldeinformationen abbrechen, wenn eine neue Anwendung festgestellt wird	Diese Option ist standardmäßig aktiviert. Steuert, ob Benutzer zum Speichern der Anmeldeinformationen aufgefordert werden, wenn der Agent eine Anwendung erkennt, für die keine Anmeldeinformationen gespeichert sind. Wenn die Option aktiviert ist, können Benutzer wählen, die Anmeldeinformationen im Anmeldungsmanager jetzt, später oder nie zu speichern. Hinweis: Wenn die Einstellung **Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern** deaktiviert ist, fordert die Agentsoftware die Benutzer nicht zum Speichern der Anmeldeinformationen auf. Weitere Informationen zu dieser Einstellung finden Sie unter „Agentverhalten konfigurieren“ auf Seite 120.
Anzahl der Tage einschränken, für die gelöschte Anmeldeinformationen verfolgt werden	Standardmäßig ist diese Option aktiviert und es sind 180 Tage eingestellt. Sie gibt an, wie lange (über wie viele Tage) der zentrale Speicher Anmeldeinformationen verfolgt, die vom Anmeldungsmanager gelöscht wurden. Wenn Anmeldeinformationen des Benutzers auf mehreren Clientgeräten gespeichert werden, löscht der Agent die Anmeldeinformationen, wenn in diesem Zeitraum eine Synchronisierung mit dem zentralen Speicher erfolgt. Wenn die Anmeldeinformationen beim Ablauf des Zeitraums immer noch auf dem Clientgerät gespeichert sind, werden sie wiederhergestellt, wenn der Agent mit dem zentralen Speicher synchronisiert wird.
Synchronisierung	
Benutzerseitiges Aktualisieren der Agenteinstellungen	Diese Option ist standardmäßig aktiviert. Steuert, ob Benutzer die Agenteinstellungen im Anmeldungsmanager aktualisieren können. Wenn die Einstellung deaktiviert ist, ist die Schaltfläche **Aktualisieren** im Anmmeldungsmanager deaktiviert.
Immer synchronisieren, wenn Benutzer erkannte Anwendungen oder den Anmeldungsmanager starten	Steuert, ob der Agent die Benutzerkonfigurationsinformationen synchronisiert, wenn ein Benutzer eine erkannte Anwendung oder Anmeldungsmanager startet. Hinweis: Häufiges Synchronisieren kann die Leistung auf dem Client und Server beeinträchtigen und den Netzwerkdatenverkehr erhöhen.

Agentausführung ohne Wiederverbindung zum zentralen Speicher zulassen	Diese Option ist standardmäßig aktiviert. Sie steuert, ob Citrix Password Manager ausgeführt wird, wenn keine Verbindung zum zentralen Speicher für die Synchronisierung hergestellt werden kann. Bei Aktivierung dieser Option wird eine lizenzierte Agentinstanz weiter ausgeführt, selbst wenn die Verbindung fehlschlägt. Bei Deaktivierung der Einstellung wird der Agent nur ausgeführt, wenn eine Verbindung zum zentralen Speicher besteht.
Zeitraum zwischen automatischen Synchronisierungsanfragen	Gibt den Zeitraum in Minuten zwischen automatischen Synchronisierungsversuchen an. Die automatische Synchronisierung hängt nicht von der Benutzeraktivität ab und wird zusätzlich zu Ereignissen ausgeführt, die eine Synchronisierung auslösen.
Zugriff auf Anmeldeinfo über das Modul 'Synchronisierung der Anmeldeinformationen' zulassen	Steuert, ob Remoteclients über dieses Dienstmodul auf die Anmeldeinformationen der Benutzer zugreifen können. Diese Option wird zusammen mit der Kontozuordnung verwendet. Mit dieser Funktion kann sich ein Agentbenutzer mit einem oder mehreren Windows-Konten an jeder Anwendung anmelden.
Kontozuordnung	
Weitere Informationen zum Konfigurieren dieser Funktion finden Sie unter „Synchronisieren von Anmeldeinformationen mit der Kontozuordnung“ auf Seite 134. Weitere Informationen finden Sie auch unter „Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen“ im *Citrix Password Manager-Installationshandbuch*.	
Anwendungsunterstützung	

Clientseitige Anwendungsdefinitionen erkennen	Diese Option ist standardmäßig aktiviert. Damit kann die Agentsoftware bestimmte clientseitige Anwendungsdefinitionen erkennen. Dazu wird eine der folgenden Optionen ausgewählt: • Alle Anwendungen: Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator oder einem Benutzer (im Anmeldungsmanager) und bei der Installation in den Standardeinstellungen definiert wurden. • Nur Anwendungen, die in Password Manager Agent eingeschlossen sind: Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator und bei der Installation in den Standardeinstellungen definiert wurden. Die Benutzer können keine eigenen Anwendungsdefinitionen im Anmeldungsmanager erstellen. • Nur Anwendungen, die von Benutzern im Anmeldungsmanager definiert sind: Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator oder einem Benutzer im Anmeldungsmanager definiert wurden. Die Agentsoftware erkennt und beantwortet keine Anfragen von Anwendungen, die bei der Installation in den Standardeinstellungen definiert wurden.
Support für Terminalemulatoren aktivieren	Steuert die Unterstützung von Terminalemulationsprogrammen. Für die Agentsoftware ist die Unterstützung von Terminalemulatoren erforderlich, um Host- oder Mainframeanwendungen zu erkennen. Bei Aktivierung der Option führt die Agentsoftware einen Prozess aus, der Terminalemulatoren erkennt. Optional können Sie einen Wert für **Zeitintervall, in dem der Agent prüft, ob Terminalemulatoränderungen aufgetreten sind** (in Millisekunden) auswählen. Diese Option gibt an, nach welchem Zeitraum die Agentsoftware prüft, ob beim Hostemulator Bildschirmänderungen aufgetreten sind. Niedrigere Werte können mehr CPU-Zeit auf dem Client belegen und den Netzwerkdatenverkehr erhöhen. Wenn die Option nicht aktiviert ist, verwendet die Agentsoftware in der Standardeinstellung 3000 Millisekunden.

Einstellungen für Webanwendungen	Gibt die Mindestanzahl der Domänennamenstufen für die Zuordnung für zulässige Webanwendungen an. Bei einem Wert von zwei oder kleiner beispielsweise wird *.domäne1.obersteDomäne zugeordnet; bei einem Wert von drei wird *.domäne2.domäne1.obersteDomäne zugeordnet. Domänennamenstufen, die über dem angegebenen Wert liegen, werden als Platzhalter behandelt. Wenn Sie die URL-Zuordnung für Webanwendungen streng steuern möchten, sollten Sie die strenge URL-Zuordnung in den Anwendungsdefinitionen einstellen.
Hotdesktop (weitere Informationen finden Sie auch unter „Einstellungen der Benutzerkonfiguration für Hotdesktop“ auf Seite 229)	
Skriptpfad für Sitzungseinstellungen	Gibt den Pfad der Datei mit den Sitzungseinstellungen an, in der die Skripts definiert sind, die am Anfang und Ende einer Hotdesktop-Sitzung ausgeführt werden. Sie können mit dem Skript am Sitzungsanfang auch Anwendungen starten. Mit dem Skript zum Beenden können Aufräumarbeiten, wie z. B. das Entfernen von Dateien, ausgeführt werden. Alle Benutzer müssen auf die Datei zugreifen können.
Sperrtimeout	Gibt den Zeitraum (in Minuten) an, für den eine Hotdesktop-Sitzung aktiv ist, wenn die Arbeitsstation im Leerlauf ist. Nach dem Ablauf des Intervalls wird der Desktop gesperrt. Der Standardwert ist 10 Minuten.
Sitzungstimeout	Gibt den Zeitraum an, für den eine Hotdesktop-Sitzung ausgeführt wird, wenn der Desktop gesperrt ist. Nach Ablauf des Zeitraums wird die Sitzung beendet, und eine neue Sitzung wird gestartet, wenn die Sperrung des Desktops aufgehoben wird. Der Standardwert ist 5 Minuten.
Sitzungsanzeige aktivieren	Diese Option ist standardmäßig aktiviert. Steuert, ob ein Fenster aktiviert ist, das die Hotdesktop-Sitzung kennzeichnet. Bei Aktivierung der Option wird in Hotdesktop-Sitzungen ein transparentes, verschiebbares Fenster auf dem Desktop angezeigt. Das Fenster gibt den Namen des Benutzers und die Dauer der aktiven Sitzung an.
Sitzungsanzeigegrafik	Gibt den Pfad der Grafikdatei an, die in der Anzeige der Hotdesktop-Sitzung angezeigt wird. Die verwendete Datei muss im Windows-Bitmap-Dateiformat (.bmp) in einem Verzeichnis gespeichert sein, auf das alle Benutzer zugreifen können.

Lizenzierung konfigurieren

Wählen Sie auf dieser Seite einen Lizenzserver und ein Lizenzierungsmodell aus. Weitere Informationen zur Lizenzierung finden Sie im Handbuch *Schnelleinstieg für die Citrix Lizenzierung*, das mit anderen Informationen zur Citrix Lizenzierung im Citrix Knowledge Center (http://support.citrix.com/licensing/) zur Verfügung steht.

Wichtig: Wenn Sie die Benutzerkonfiguration nachträglich bearbeiten und die Produktedition ändern, ändert sich auch das Lizenzierungsmodell. Wenn Sie zum Beispiel die Produktedition von Password Manager Enterprise in Password Manager Advanced ändern, ändert sich das Lizenzierungsmodell von „Gleichzeitige Benutzer“ in „Benannter Benutzer“.

- **Name des Lizenzservers**

  Geben Sie in dieses Feld den vollqualifizierten Domänennamen des Lizenzservers ein.

- **Portnummer**

  Sie können die Standard-Portnummer 27000 auswählen, indem Sie das Kontrollkästchen **Standard verwenden** aktivieren.

- **Benannte Benutzer-Lizenzierung**

  Diese Option ist aktiviert, wenn Sie diesen Lizenztyp erworben haben und als Produktedition Password Manager Advanced ausgewählt haben. Sie können diese Option auch auswählen, wenn Sie als Produkteditionen Presentation Server Platinium oder Password Manager Enterprise einstellen.

  Mit diesem Lizenztyp kann Password Manager nur von bestimmten, benannten Benutzern verwendet werden.

  - **Zeitraum für getrennten Modus**

    Geben Sie an, für welchen Zeitraum die Lizenz dem benannten Benutzer zugeordnet ist. Danach läuft die Lizenz ab, und die Agent-software stellt eine neue Verbindung zum Lizenzserver her. Die Lizenz wird für diesen Zeitraum verbraucht, selbst wenn der Benutzer den PC abschaltet. Der Standardzeitraum ist 21 Tage. Weitere Informationen finden Sie auch in der Beschreibung zur Synchronisierungseinstellung **Ausführen des Agents zulassen, wenn Wiederverbindung mit dem zentralen Speicher unmöglich ist** unter „Erweiterte Einstellungen“ auf Seite 122.

- **CCU-Lizenzierung (nur Enterprise und Platinum Edition)**

  Diese Option ist aktiviert, wenn Sie als Produkteditionen Presentation Server Platinium oder Password Manager Enterprise auswählen. Bei Auswahl von Password Manager Advanced als Produktedition ist die Option deaktiviert.

  Hinweis: Dieses Lizenzierungsmodell ist aktiviert, wenn Sie von den Password Manager Version 4.1 aktualisiert haben. In Bezug auf die Lizenzierung betrachtet Citrix System beim Upgrade diese frühere Version als gleichwertig zu Password Manager 4.6 Enterprise Edition.

  Mit diesem Lizenztyp kann eine einzelne Password Manager-Lizenz von mehreren Benutzern gemeinsam verwendet werden (jedoch nicht gleichzeitig). Dieser Lizenztyp wird auch als Lizenzierungsmodell *Gleichzeitige Benutzer* bezeichnet.

  - **Lizenzverbrauch für Offlineverwendung zulassen**

    Aktivieren Sie diese Option, um die Dauer anzugeben, für die der Benutzer offline sein kann, bevor die Lizenz abläuft und in den Pool der verfügbaren Lizenzen zurückgegeben wird. Bei Aktivierung wird die Lizenz für diesen Zeitraum verbraucht, selbst wenn der Benutzer den PC abschaltet. Die Standardeinstellung für den Zeitraum ist 21 Tage; Werte zwischen zwei und 365 Tagen sind zulässig.

    Wenn diese Option nicht ausgewählt ist, läuft die Lizenz nach 1 Stunde und 30 Minuten ab und wird an den Pool zurückgegeben. Dieser Zeitraum kann nicht eingestellt werden.

    Weitere Informationen hierzu finden Sie in der Beschreibung zur Synchronisierungseinstellung **Ausführen des Agents zulassen, wenn Wiederverbindung mit dem zentralen Speicher unmöglich ist** unter „Erweiterte Einstellungen“ auf Seite 122.

Datenschutzmethoden auswählen

Auf dieser Seite können Sie die Datenschutzmethoden zum Schutz der Anmeldeinformationen der Benutzer auswählen, je nachdem, welche der Authentifizierungsmethoden die Benutzer verwenden dürfen. In einigen Umgebungen können die Benutzer mehrere Methoden verwenden. Weitere Informationen finden Sie unter „Verwenden der Identitätsprüfung“ und „Planen der Benutzerkonfigurationen“ im *Citrix Password Manager-Installationshandbuch* und unter „Benutzerseitiges Wechseln zwischen Authentifizierungsmethoden“ auf Seite 157.

Hinweis: Wenn Sie den zentralen Speicher von Password Manager von Version 4.1 auf Version 4.6 aktualisiert haben, ist die Option **Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden** automatisch aktiviert.

Wichtig: Für die Verwendung von Smartcards unter Windows Vista müssen Sie die Option **Microsoft Data Protection API** in den Benutzerkonfigurationen aktivieren.

- **Administratorkontozugriff auf Benutzerdaten steuern**

  Wählen Sie **Ja** aus, wenn Sie verhindern möchten, dass Administratoren auf die Anmeldeinformationen der Benutzer zugreifen dürfen.

  Ja ist die Standardeinstellung auf dieser Seite. Mit dieser Konfiguration haben Administratoren, wie z. B. der Kontoadministrator, keinen Zugriff auf die Benutzerkennwörter oder die Benutzerdaten. Mit dieser Einstellung kann verhindert werden, dass ein Administrator die Identität eines Benutzers annimmt. Mit der Standardeinstellung kann sich der Administrator nicht als der Benutzer an der Agentsoftware anmelden und möglicherweise auf Daten zugreifen, die sich im lokalen Speicher der Anmeldeinformationen des Benutzers befinden.

  Wenn Sie **Ja** auswählen, sind sowohl die Optionen unter **Microsoft Data Protection API** (einschließlich der Auswahl **DPAPI mit Profil** im Dropdownmenü **Smartcardschlüsselquelle**) auf dieser Seite als auch die Option **Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt** auf der folgenden Seite **Sekundäre Datenschutzoptionen auswählen** deaktiviert.

Wählen Sie **Nein** aus, wenn Sie die Verwendung der verschiedenen Authentifizierungsfunktionen auf dieser Seite sowie der sekundären Datenschutzmethoden auf der folgenden Seite im Assistenten (weitere Informationen hierzu finden Sie unter „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132) ermöglichen möchten.

- **Wählen Sie alle in Frage kommenden Datenschutzmethoden aus, um dem Benutzer die Anmeldung zu erleichtern.**

Mit dieser Auswahl können Sie die verschiedenen primären Authentifizierungsfunktionen in dieser Version von Password Manager verwenden und das Verhalten der Agentsoftware steuern. Zu den Optionen gehören u. a.:

Authentifizierungs-daten der Benutzer	Zum Zugreifen auf die Benutzerdaten und den Datenschutz wird ein „Geheimnis“ verwendet. Bei diesem Geheimnis zur Authentifizierung kann es sich um ein Benutzerkennwort oder ein PIN-basiertes Gerät in der Umgebung handeln. Außerdem stehen die folgenden Optionen zum Datenschutz zur Verfügung: **Smartcard-PINs zulassen** Aktivieren Sie diese Option, um die Verwendung von Smartcard-PINs als Geheimnis zum Datenschutz zu ermöglichen. Verwenden Sie diese Option nur, wenn das Unternehmen oder die Umgebung eine „starke PIN-Richtlinie“ hat. **Schutz mit leeren Kennwörtern zulassen** Aktivieren Sie diese Option nur, wenn die Sicherheitsanforderungen in der Domäne gering sind und die Benutzer leere Domänenkennwörter verwenden dürfen. Wenn diese Option aktiviert ist und die Agentsoftware erkennt, dass der Benutzer ein leeres Kennwort hat, wird aus der Benutzerkennung ein Geheimnis abgeleitet. Wenn Sie diese Option nicht aktivieren, leitet die Agentsoftware kein Geheimnis ab und führt auch keine anderen Datenschutzmaßnahmen mit dem leeren Kennwort aus. Wenn Sie die Option **Authentifizierungsdaten der Benutzer** aktivieren, die Optionen **Smartcard-PINs zulassen** und **Schutz mit leeren Kennwörtern zulassen** jedoch nicht, wird eine Fehlermeldung angezeigt, wenn sich der Benutzer zur Erstregistrierung mit einem leeren Kennwort anmeldet, und die Agentsoftware wird deaktiviert.

Microsoft Data Protection API	Aktivieren Sie diese Option, wenn Sie servergespeicherte Profile mit einem Kerberos-Netzwerkauthentifizierungsprotokoll für die Benutzer verwenden. Diese Option funktioniert nur, wenn servergespeicherte Profile verfügbar sind. Sie können die Option **Authentifizierungsdaten der Benutzer** sowie diese Option zum Beispiel dann aktivieren, wenn die Benutzer mit Kennwörtern auf die PCs und mit einem Kerberos-Netzwerk-authentifizierungsprotokoll auf eine Farm mit Citrix Presentation Server zugreifen. Mit dieser Methode können Benutzer sich auch mit Anmeldeinformationen und Smartcards anmelden.
Smartcardzertifikat	Aktivieren Sie diese Option, um den Benutzern die Verwendung von kryptographischen Karten zu erlauben, mit denen Authentifizierungsdaten verschlüsselt und entschlüsselt werden. Citrix empfiehlt, diese Option möglichst bei Verwendung von Hotdesktop in der Umgebung zu aktivieren.

- **Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden**

  Aktivieren Sie diese Option und wählen Sie aus dem Dropdownmenü **Smartcardschlüsselquelle** eine Methode aus, wenn die Benutzer eine einzelne primäre Authentifizierungsmethode verwenden können sollen und/oder Sie die Version 4.0 oder 4.1 der Agentsoftware verwenden. Wenn Sie den zentralen Speicher von Password Manager von Version 4.1 auf Version 4.6 aktualisiert haben, ist diese Option automatisch aktiviert.

  - PIN-Nummer als Kennwort
  - Smartcard-Datenschutz
  - **DPAPI mit Profil** (nicht verfügbar wenn Sie **Nein** für **Administratorkontozugriff auf Benutzerdaten steuern** ausgewählt haben

Sekundäre Datenschutzoptionen auswählen

Für den Fall, dass ein Benutzer seine primäre Authentifizierung ändert (z. B. Änderung des Domänenkennworts oder Austausch der Smartcard), können Sie auf dieser Seite die Optionen für den Datenschutz mit sekundären Anmeldeinformationen festlegen, die verwendet werden, bevor die Sperre der Anmeldeinformationen des Benutzers aufgehoben wird. Hier können Sie auch einstellen, dass die Benutzer ihre Identität nachweisen müssen, um eine höhere Sicherheit zu gewährleisten.

Alternativ können Sie einstellen, dass Anmeldeinformationen automatisch wiederhergestellt werden. Dazu wird das Schlüsselverwaltungsmodul implementiert.

- **Benutzeridentität prüfen**

  Aktivieren Sie dieses Optionsfeld, um eine der folgenden Methoden zur Neuauthentifizierung der Benutzer auszuwählen:

Benutzer zur Eingabe des alten Kennworts auffordern	Beachten Sie, dass Benutzer, die ihr Kennwort vergessen, ausgesperrt werden und sich mit den sekundären Anmeldeinformationen neu registrieren müssen, wenn Sie diese Option aktivieren. Aktivieren Sie diese Option nicht, wenn die Benutzer Smartcards für die primäre Authentifizierung einsetzen.
Benutzerseitige Auswahl der Methode: Altes Kennwort oder Sicherheitsfragen	Wenn Sie diese Option aktivieren, werden die Benutzer aufgefordert, sich mit der von ihnen ausgewählten Methode zu authentifizieren. Diese Option enthält diese Unteroption: Identitätsprüfung wie in vorherigen Password Manager-Versionen Aktivieren Sie diese Option, wenn Sie von Password Manager Version 4.0 oder 4.1 aktualisiert und die fragenbasierte Authentifizierung oder Fragen zur Identitätsprüfung aktiviert haben. In diesem Fall müssen die Versionen 4.0 und 4.1 der Agentsoftware nicht auf den Dienst zugreifen.

- **Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul)**

  Aktivieren Sie diese Option, wenn Sie das Modul **Schlüsselverwaltung** zum Auslassen der Identitätsprüfung und zum automatischen Aufheben der Sperrung der Anmeldeinformationen der Benutzer implementieren. Diese Methode ist weniger sicher als andere Datenschutzmethoden, jedoch benutzerfreundlicher, da die Anmeldeinformationen automatisch abgerufen werden.

Self-Service-Funktionen aktivieren

Für die auf dieser Seite zur Verfügung stehenden Optionen muss das Modul **Schlüsselverwaltung** installiert werden. Durch diese Funktion wird das Windows-Anmeldedialogfeld um die Schaltfläche **Konto-Self-Service** erweitert, mit der die Administrationskosten oder die Kosten für die Unterstützung durch den Helpdesk im Unternehmen gesenkt werden können.

Mit diesen Optionen können Benutzer, die ihr Kennwort vergessen haben, das primäre Domänenkennwort zurücksetzen und die Sperrung des Domänenkontos aufheben, ohne sich an den Helpdesk wenden zu müssen.

Die folgenden Optionen stehen zur Auswahl:

- **Benutzerseitiges Zurücksetzen des primären Domänenkennworts**
- **Benutzerseitiges Aufheben der Sperrung des Domänenkontos**

Dienstmodule suchen

Auf diesen Seiten müssen Sie die URL und den Dienstport aller installierten Dienstmodule angeben. Weitere Informationen finden Sie unter „Auswählen optionaler Funktionen des Password Manager-Dienstes“ und „Installieren und Konfigurieren des Password Manager-Dienstes“ im *Citrix Password Manager-Installationshandbuch*.

1. Wählen Sie die Optionen für die einzelnen Dienstmodule aus.
2. Geben Sie den vollqualifizierten Domänennamen des PCs, auf dem der Dienst ausgeführt wird, und die Portnummer an. (Die Standard-Portnummer ist 443.) Weitere Informationen finden Sie unter „Portnummer für den Password Manager-Dienst“ im *Citrix Password Manager-Installationshandbuch*.

Beenden des Assistenten für Benutzerkonfigurationen

1. Prüfen Sie die Einstellungen auf der Seite **Einstellungen bestätigen**.

   Klicken Sie auf **Zurück**, um eine Einstellung zu ändern.

2. Klicken Sie auf der Seite **Einstellungen bestätigen** auf die Schaltfläche **Fertig stellen**, um die Benutzerkonfiguration zu erstellen.

Synchronisieren von Anmeldeinformationen mit der Kontozuordnung

Wie im *Citrix Password-Installationshandbuch* unter „Verwenden der Kontozuordnung mit mehreren zentralen Speichern und Kontoanmeldeinformationen der Benutzer in einem Unternehmen mit mehreren Domänen" beschrieben, haben Benutzer in Unternehmen mit mehreren Windows-Domänen auch mehrere Windows-Konten. Password Manager enthält für die Aktivierung der Kontozuordnung den Dienst **Synchronisierung der Anmeldeinformationen**.

Mit der Kontozuordnung kann sich ein Agentbenutzer mit jedem Windows-Konto an jeder Anwendung anmelden. Da Password Manager normalerweise Anmeldeinformationen des Benutzers mit einem Konto verbindet, werden die Anmeldeinformationen nicht automatisch zwischen mehreren Konten des Benutzers synchronisiert. Administratoren können jedoch die Kontozuordnung konfigurieren und die Anmeldeinformationen des Benutzers synchronisieren. Benutzer, für die die Kontozuordnung konfiguriert ist, können mit jedem ihrer Konten in der Password Manager-Umgebung auf alle Anwendungen zugreifen. Wenn die Anmeldeinformationen des Benutzers geändert, hinzugefügt oder von einem Konto entfernt werden, werden die Anmeldeinformationen automatisch mit jedem zugeordneten Konto des Benutzers synchronisiert.

Ohne die Kontozuordnung muss ein Benutzer, der mehrere Windows-Konten besitzt, die Anmeldeinformationen manuell für jedes Windows-Konto ändern.

Konfigurieren der Kontozuordnung

Für die Konfiguration der Kontozuordnung müssen Windows-Domänenadministratoren des Unternehmens die folgenden Schritte der Reihe nach ausführen:

Aufgabe	Siehe Abschnitt
1. Wählen Sie eine Domäne, in der Sie das Modul **Synchronisierung der Anmeldeinformationen** installieren und ausführen, das Teil des Password Manager-Dienstes ist.	• „Auswählen und Konfigurieren einer Domäne für das Modul „Synchronisierung der Anmeldeinformationen““ auf Seite 135 • „So konfigurieren Sie die Synchronisierung der Anmeldeinformationen in der Hostdomäne“ auf Seite 136
2. Stellen Sie das vertrauenswürdige Stammzertifikat allen Computern im Unternehmen bereit, die die Kontozuordnung verwenden.	“Anforderungen für das Serverauthentifizierungszertifikat“ im *Citrix Password Manager-Installationshandbuch*.
3. Synchronisieren Sie manuell alle Anwendungsdefinitionen zwischen den Domänen.	„So synchronisieren Sie manuell alle Anwendungsdefinitionen zwischen den Domänen“ auf Seite 137
4. Konfigurieren Sie die Benutzereinstellungen für die Kontozuordnung in anderen Domänen, die mit dem Modul **Synchronisierung der Anmeldeinformationen** verbunden sind.	„So konfigurieren Sie Benutzereinstellungen für die Kontozuordnung in anderen Domänen“ auf Seite 137
5. Die Kontozuordnung muss von jedem Benutzer in der Agentsoftware aktiviert werden.	• „Konfigurieren der Kontozuordnung in der Agentsoftware“ auf Seite 139 • „So konfigurieren Sie die Kontozuordnung in der Agentsoftware“ auf Seite 139

Auswählen und Konfigurieren einer Domäne für das Modul „Synchronisierung der Anmeldeinformationen“

Wählen Sie die Domäne, die die Konten aller Benutzer im Unternehmen enthält, die die Kontozuordnung verwenden. Das Modul **Synchronisierung der Anmeldeinformationen** agiert als Netzknoten für alle Anmeldeinformationen im Unternehmen. Installieren Sie dieses Modul wie einen Password Manager-Dienst in dieser Domäne. Weitere Informationen finden Sie unter „Installieren und Konfigurieren des Password Manager-Dienstes“ im *Citrix Password Manager-Installationshandbuch*.

Wichtig: Wenden Sie sich an den Netzwerkadministrator, um festzustellen, ob Firewalländerungen erforderlich sind, und ob diese Änderungen die Unternehmensrichtlinien einhalten.

Erstellen oder bearbeiten Sie nach der Installation des Moduls **Synchronisierung der Anmeldeinformationen** Benutzerkonfigurationen in der Password Manager Console, um einzelnen Benutzerkonten die Berechtigung zur Verwendung des Moduls **Synchronisierung der Anmeldeinformationen** zu erteilen, wie im folgenden Abschnitt beschrieben.

So konfigurieren Sie die Synchronisierung der Anmeldeinformationen in der Hostdomäne

---

Hinweis: Öffnen Sie die Konsole von der Domäne, die das Modul **Synchronisierung der Anmeldeinformationen** hostet. Einige Domänen können auf mehrere zentrale Speicher zugreifen. Stellen Sie sicher, dass die Konsole, die Sie verwenden, eine Verbindung zu demselben zentralen Speicher wie das Modul **Synchronisierung der Anmeldeinformationen** herstellt.

---

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie eine vorhandene Benutzerkonfiguration aus oder erstellen Sie eine neue.
   - Zum Erstellen einer neuen Benutzerkonfiguration sind die folgenden Optionen auf der Seite **Agentverhalten konfigurieren** über die Schaltfläche **Erweiterte Einstellungen** verfügbar.
   - Zum Bearbeiten einer vorhandenen Benutzerkonfiguration stehen die folgenden Optionen auf der Eigenschaftenseite **Benutzerkonfiguration bearbeiten** zur Verfügung.
4. Klicken Sie auf **Synchronisierung** und aktivieren Sie das Kontrollkästchen **Zugriff auf Anmeldeinfo über das Modul „Synchronisierung der Anmeldeinformationen“ zulassen**.
5. Klicken Sie auf **OK** und wiederholen Sie diese Schritte für jede vorhandene oder neue Benutzerkonfiguration.

So synchronisieren Sie manuell alle Anwendungsdefinitionen zwischen den Domänen

Hinweis: Konten können auch synchronisiert werden, wenn die Benutzerkonfigurationen unterschiedlich zugeordnet sind. Sie können z. B. eine Benutzerkonfiguration in einer Domäne einer Active Directory-Hierarchie (OU oder Benutzer) und in einer anderen Domäne einer Active Directory-Gruppe zuordnen. Solange die Namen der Anwendungsdefinitionen in jeder Benutzerkonfiguration identisch sind, werden die Anmeldeinformationen mit der Kontozuordnung synchronisiert.

Anmeldeinformationen der Benutzer werden nur für Anwendungen gemeinsam verwendet, die vom Password Manager-Administrator definiert wurden. Administratoren müssen sicherstellen, dass jede Anwendungsdefinition in jeder Domäne denselben Namen in jedem zentralen Speicher hat.

Beispiel: Wenn die Anwendungsdefinition für SAP in einer Domäne **SAP-Anmeldung** heißt, **SAP** in einer anderen Domäne und **SAP Launch Pad** in einer weiteren, werden die Anmeldeinformationen des Benutzers nicht für diese Anwendungen zwischen den Konten für diese Domäne synchronisiert.

Bei der Erstellung einer neuen domänenübergreifenden Anwendungsdefinition verwenden Sie am besten die Tasks **Administrative Daten exportieren** und **Administrative Daten importieren** in der Konsole. Mit diesen Tasks exportieren Sie gerade erstellte Anwendungsdefinitionen, die Sie in jeden zentralen Speicher importieren. Bestehende, bereits definierte Anwendungen müssen manuell umbenannt werden.

So konfigurieren Sie Benutzereinstellungen für die Kontozuordnung in anderen Domänen

Hinweis: Installieren und öffnen Sie die Konsole auf einer Arbeitsstation in jeder Domäne, die das Modul **Synchronisierung der Anmeldeinformationen** nicht hostet. Einige Domänen haben mehrere zentrale Speicher. Stellen Sie daher sicher, dass Sie jeden zentralen Speicher konfigurieren.

Alle Domänenadministratoren müssen die Domänenbenutzer berechtigen, die Konten ihrem Hostdomänenkonto zuzuordnen. Bearbeiten Sie in der Konsole den Abschnitt **Kontozuordnung** für die entsprechenden Benutzerkonfigurationen.

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.

2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie eine vorhandene Benutzerkonfiguration aus oder erstellen Sie eine neue.
    - Zum Erstellen einer neuen Benutzerkonfiguration sind die folgenden Optionen auf der Seite **Agentverhalten konfigurieren** über die Schaltfläche **Erweiterte Einstellungen** verfügbar.
    - Zum Bearbeiten einer vorhandenen Benutzerkonfiguration stehen die folgenden Optionen auf der Eigenschaftenseite **Benutzerkonfiguration bearbeiten** zur Verfügung.
4. Klicken Sie auf **Kontozuordnung**.
5. Aktivieren Sie die Option **Benutzer können Konten zuordnen**.

    Die folgenden Optionen sind nicht erforderlich, ergeben jedoch eine nahtlose Benutzererfahrung.
6. Aktivieren Sie die Option **Standarddienstadresse angeben** und geben Sie die Adresse und den Port des Password Manager-Dienstes für die Domäne an, die das Modul **Synchronisierung der Anmeldeinformationen** hostet.
7. Deaktivieren Sie die Option **Benutzer können die Dienstadresse bearbeiten**.
8. Aktivieren Sie die Option **Standarddomäne angeben** und geben Sie den Namen der Domäne ein, die das Modul Synchronisierung der Anmeldeinformationen hostet.

    Hinweis: Wenn Sie die Domäne nicht angeben, wissen die Benutzer möglicherweise nicht, welche Anmeldeinformationen für welches Domänenkonto eingegeben werden sollen.

    ---
9. Deaktivieren Sie die Option **Benutzer können die Domäne bearbeiten**.
10. Aktivieren Sie die Option **Benutzer können das Kennwort speichern**, wenn die Sicherheitsrichtlinien des Unternehmens dies zulassen.
11. Klicken Sie auf **OK**. Wiederholen Sie die Schritte für jede Benutzerkonfiguration.

Nach der Durchführung der erwähnten Schritte können Benutzer die Windows-Konten zuordnen.

Konfigurieren der Kontozuordnung in der Agentsoftware

Bei der Anmeldung an der Domäne, die das Modul **Synchronisierung der Anmeldeinformationen** hostet, müssen Benutzer nichts für die Aktivierung der Kontozuordnung tun. Diese Konten agieren als zentrales Repository für die Anmeldeinformationen jedes Benutzers.

Bei der Anmeldung an anderen Domänen wird den Benutzern im Menü **Extras** in der Agentsoftware die Option **Kontozuordnung** angezeigt. Benutzer müssen mit dieser Option die Kontozuordnung konfigurieren.

So konfigurieren Sie die Kontozuordnung in der Agentsoftware

1. Tun Sie Folgendes:

   - Wählen Sie vom Symbol für Password Manager Agent im Infobereich **Extras** > **Kontozuordnung**.
   - Wählen Sie im Anmeldungsmanager **Extras** > **Kontozuordnung**.

   Das Dialogfeld **Kontozuordnung** wird angezeigt.

2. Aktivieren Sie die Option **Kontozuordnung aktivieren**.

Hinweis: Wenn Sie die Dienstadresse für das Modul **Synchronisierung der Anmeldeinformationen** nicht angegeben haben, müssen die Benutzer die Adresse im Textfeld eingeben. Wenn das Feld nicht verfügbar ist, haben Sie diese Dienstadresse bereits bereitgestellt und die Benutzer können keinen Text in dieses Feld eingeben. Weitere Informationen finden Sie unter „So konfigurieren Sie Benutzereinstellungen für die Kontozuordnung in anderen Domänen“ auf Seite 137.

---

3. Klicken Sie auf **OK**.

   Das Dialogfeld **Für die Kontozuordnung authentifizieren** wird angezeigt.

4. Geben Sie den Benutzernamen und das Kennwort für ihr zugeordnetes Windows-Konto ein.

   Wenn die Domäne, in der das Modul zur Synchronisierung der Anmeldeinformationen installiert ist, nicht angezeigt wird, geben Sie den Wert in das Feld **Domäne** ein.

   Hinweis: Wenn Sie den Domänennamen eingegeben haben, können die Benutzer keinen Text in dieses Feld eingeben. Weitere Informationen finden Sie unter „So konfigurieren Sie Benutzereinstellungen für die Kontozuordnung in anderen Domänen“ auf Seite 137.

   ---

5. Klicken Sie auf **OK**.

   Die Kontozuordnung ist konfiguriert. Die Anmeldeinformationen des Benutzers werden bei der Agentsynchronisierung synchronisiert.

Zurücksetzen und Löschen von Benutzerdaten

Password Manager bietet zwei Benutzerkonfigurationstasks zum Verwalten von Änderungen in der Umgebung und im Unternehmen:

- „Benutzerdaten zurücksetzen“ auf Seite 141
- „Benutzerdaten aus dem zentralen Speicher löschen“ auf Seite 143

Benutzerdaten zurücksetzen

Hinweis: Für den Task **Benutzerdaten zurücksetzen** muss das Modul **Provisioning** installiert und konfiguriert sein.

Mit dem Task **Benutzerdaten zurücksetzen** können Sie Benutzerdaten im zentralen Speicher zurücksetzen, wodurch der ausgewählte Benutzer auf den Originalzustand zurückgesetzt wird.

- In zentralen Speichern unter Active Directory werden die Benutzerdaten (Anmeldeinformationen, Sicherheitsfragen und Antworten usw.) gelöscht, und der Benutzer wird als zurückgesetzt gekennzeichnet.
- In zentralen Speichern auf einer NTFS-Netzwerkfreigabe oder in einem freigegebenen Novell Ordner werden alle Benutzerdaten gelöscht, und der Benutzer wird als zurückgesetzt gekennzeichnet.

Sie können die Funktion **Benutzerdaten zurücksetzen** verwenden, wenn ein Benutzer die Antworten auf seine Sicherheitsfragen vergisst oder die Anmeldeinformationen eines Benutzers zurückgesetzt werden müssen, weil die Daten des Benutzers beschädigt wurden. Wenn sich der betreffende Benutzer später an der Agentsoftware anmeldet, um eine Verbindung zum zentralen Speicher herzustellen, sind im lokalen Speicher der Anmeldeinformationen des Benutzers keine Daten mehr enthalten und der Benutzer muss sich wie bei der Ersteinrichtung der Anmeldeinformationen erneut registrieren.

Dieser Task kann auch verwendet werden, wenn sich ein Benutzer nicht am Agent anmelden kann.

Wichtig: Der Kennwortverlauf wird pro Benutzer gespeichert. Wenn Sie die Benutzerdaten für einen Benutzer zurücksetzen, wird der Kennwortverlauf entfernt, und der Kennwortverlauf kann nicht für die gelöschten Kennwörter erzwungen werden.

So setzen Sie Benutzerdaten zurück

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Klicken Sie unter **Andere Tasks** auf **Benutzerdaten zurücksetzen**.

   Das Dialogfeld **Benutzer auswählen** wird angezeigt.
4. Geben Sie einen Benutzernamen in das Textfeld ein und klicken Sie auf **Namen überprüfen**.
5. Wenn der Benutzer gefunden wurde, klicken Sie auf **OK**.
6. Wählen Sie einen Benutzer im zentralen Speicher aus und klicken Sie auf **Zurücksetzen**.
7. Klicken Sie auf **OK**.

   Eine Warnmeldung wird angezeigt.
8. Stellen Sie sicher, dass alle Benutzer, die Password Manager als eine unter Citrix Presentation Server ausgeführte Anwendung ausführen, abgemeldet sind und klicken Sie auf **Weiter**, um die Daten des Benutzers für das Zurücksetzen zu markieren.

   Wenn nicht alle Benutzer abgemeldet sind, klicken Sie auf **Abbrechen**, setzen Sie die ICA-Sitzungen zurück und fahren Sie mit diesem Verfahren fort.
9. Klicken Sie im Dialogfeld **Benutzerdaten zurücksetzen** auf **OK**, wenn die Benutzerdaten geprüft und zurückgesetzt wurden.

   Die Daten des Benutzers werden zurückgesetzt, wenn er sich das nächste Mal mit der Agentsoftware an Password Manager anmeldet.

Benutzerdaten aus dem zentralen Speicher löschen

Mit dem Task **Benutzerdaten aus dem zentralen Speicher löschen** werden alle Benutzerdaten aus dem zentralen Speicher gelöscht. Sie können den Task **Benutzerdaten aus dem zentralen Speicher löschen** zum Beispiel verwenden, wenn ein Benutzer das Unternehmen endgültig verlässt.

Der lokale Speicher der Anmeldeinformationen auf dem PC des Benutzers bleibt bestehen, bis er von einem Administrator oder Operator gelöscht wird.

Hinweis: Wenn der gelöschte Benutzer die Agentsoftware ausführt, wird der lokale Speicher der Anmeldeinformationen der Agentsoftware mit dem zentralen Speicher synchronisiert, es sei denn, der lokale Speicher der Anmelde-informationen wurde von einem Administrator oder Operator gelöscht. Und dies zu verhindern, sollten Sie den Benutzer aus dem Unternehmen löschen (z. B. aus Active Directory löschen oder deaktivieren).

So löschen Sie Benutzerdaten

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Klicken Sie unter **Andere Tasks** auf **Benutzerdaten aus dem zentralen Speicher löschen**.

   Das Dialogfeld **Benutzer auswählen** wird angezeigt.
4. Geben Sie einen Benutzernamen in das Textfeld ein und klicken Sie auf **Namen überprüfen**.
5. Wenn der Benutzer gefunden wurde, klicken Sie auf **OK**. Klicken Sie zur Bestätigung auf **Ja**.

   Eine Warnmeldung wird angezeigt.
6. Klicken Sie auf **OK**.

   Der Benutzer wird aus dem zentralen Speicher gelöscht.

Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen

Sie können einstellen, dass ein bestimmter Benutzer oder alle Benutzer die Antworten auf die Sicherheitsfragen neu registrieren müssen. Diese Funktionen werden aus Sicherheitsgründen oder bei beschädigten Benutzerdaten verwendet.

- **Die Registrierung der Sicherheitsfragen für einen Benutzer aufheben**

  Aktivieren Sie diese Option, um die Daten zu den Sicherheitsfragen eines Benutzers zu löschen. Die fragenbasierte Authentifizierung steht danach erst wieder zur Verfügung, wenn der Benutzer eine Neuregistrierung vorgenommen hat.

- **Alle Benutzer zur Neuregistrierung der Sicherheitsfragen auffordern**

  Aktivieren Sie diese Option, um einzustellen, dass alle Benutzer die Sicherheitsfragen und Antworten neu registrieren müssen, wenn sie die Agentsoftware starten. Die Daten zu den Sicherheitsfragen bleiben erhalten und die Benutzer können mit den aktuellen Antworten noch auf die Funktionen zugreifen, die eine fragenbasierte Authentifizierung erfordern. Die Benutzer werden wiederholt zur Neuregistrierung aufgefordert, bis sie diese Aktion ausführen.

Hinweis: Wenn sich ein Benutzer gegen die Neuregistrierung seiner Antworten entscheidet, indem er im Dialogfeld **Citrix Password Manager-Registrierung** auf **Abbrechen** klickt, kann er bis zur Neuregistrierung seiner Antworten keine Funktionen mehr verwenden, die eine fragenbasierte Authentifizierung erfordern, wie z. B. Konto-Self-Service.

So fordern Sie die Benutzer zur Neuregistrierung auf

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Aktivieren Sie eine der folgenden Optionen:

   - **Die Registrierung der Sicherheitsfragen für einen Benutzer aufheben**

     Das Dialogfeld **Benutzer auswählen** wird angezeigt. Geben Sie einen Benutzer ein oder wählen Sie ihn aus. Bestätigen Sie, dass Sie die Registrierung der Sicherheitsfragen für diesen Benutzer zurücksetzen möchten.

   - **Alle Benutzer zur Neuregistrierung der Sicherheitsfragen auffordern**

     Klicken Sie auf **Ja**, um alle Benutzer aufzufordern, und klicken Sie dann auf **OK**.

Zuweisen von Prioritäten zu Benutzerkonfigurationen

Beim Erstellen oder Bearbeiten einer Benutzerkonfiguration können Sie Benutzer, die zu Active Directory-Gruppen gehören, Benutzerkonfigurationen zuordnen. Ein Benutzer in einer Gruppe kann mehreren Benutzerkonfigurationen zugeordnet sein. In einem solchen Fall können Sie festlegen, welche Benutzerkonfiguration die höchste Priorität hat.

Wichtig: Die Organisation der Password Manager-Benutzerumgebung kann sich auf die Funktion der Benutzerkonfigurationen auswirken. Das heißt, dass Benutzerkonfigurationen in der Password Manager-Umgebung einer Active Directory-Hierarchie (OU oder Benutzer) oder einer Active Directory-Gruppe zugeordnet werden. Wenn Sie sowohl Hierarchien als auch Gruppen verwenden und ein Benutzer beiden zugeordnet ist, hat die einer Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung.

So legen Sie die Priorität einer Benutzerkonfiguration fest

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Klicken Sie auf **Priorität für Benutzerkonfiguration festlegen**.

   Das Dialogfeld **Priorität für Benutzerkonfiguration festlegen** wird angezeigt.
4. Wählen Sie eine Benutzerkonfiguration aus und klicken Sie je nach gewünschter Einstellung auf **Auf** oder **Ab**.
5. Klicken Sie auf **OK**.

Zuweisen einer Benutzerkonfiguration zu verschiedenen Benutzern

Beachten Sie, dass Sie beim Bearbeiten einer vorhandenen Benutzer-konfiguration nicht den Speicherort der Benutzerkonfiguration verändern können. Sie können einen der folgenden Vorgänge ausführen:

- Anwenden einer Benutzerkonfiguration auf zusätzliche Benutzer durch Duplizierung der Benutzerkonfiguration
- Anwenden einer Benutzerkonfiguration auf andere Benutzer durch Verschieben der Benutzerkonfiguration

So duplizieren Sie eine Benutzerkonfiguration

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie die Benutzerkonfiguration aus.
4. Klicken Sie auf **Benutzerkonfiguration duplizieren**.
5. Geben Sie einen Namen für die duplizierte Konfiguration ein.
6. Geben Sie die OU, den Benutzer oder die Gruppe an, zu der/dem die Benutzer gehören, für die die Benutzerkonfiguration gelten soll.
7. Klicken Sie auf **OK**.

So verschieben Sie eine Benutzerkonfiguration zu anderen Benutzern

Hinweis: Eine Benutzerkonfiguration, die einer Active Directory-Gruppe zugeordnet ist, kann nicht verschoben werden. Zum Zuordnen der Benutzerkonfiguration zu einer Active Directory-Hierarchie (OU oder Benutzer) duplizieren Sie die Benutzerkonfiguration und geben Sie die gewünschte Zuordnung an. Weitere Informationen finden Sie unter „So duplizieren Sie eine Benutzerkonfiguration“ auf Seite 147.

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie die Benutzerkonfiguration aus.
4. Klicken Sie auf **Benutzerkonfiguration verschieben**.
5. Geben Sie die OU, den Benutzer oder die Gruppe an, zu der/dem die Benutzer gehören, für die die Benutzerkonfiguration gelten soll.
6. Klicken Sie auf **OK**.

Aktualisieren vorhandener Benutzerkonfigurationen

In den Versionen 4.0 und 4.1 von Citrix Password Manager wurden die Benutzer über eine Active Directory-Hierarchie (OU oder Benutzer) einer Benutzerkonfiguration zugeordnet. In der Version 4.5 können Benutzer auch über eine Active Directory-Gruppe zugeordnet werden.

Beachten Sie die folgenden Punkte, wenn Sie vorhandene Benutzerkonfigurationen aktualisieren möchten, deren Benutzer einer Active Directory-Hierarchie zugeordnet sind:

- Wenn Sie eine vorhandene Benutzerkonfiguration verwenden, die nach Hierarchie organisiert ist, und nun Benutzerkonfigurationen erstellen, die Gruppen zugeordnet sind, und ein Benutzer beiden zugeordnet ist, hat die der Hierarchie zugeordnete Benutzerkonfiguration Vorrang und wird verwendet. Bei einer solchen Konstellation spricht man von einer gemischten Umgebung. In dieser Situation stellen die Benutzer ggf. ein unerwartetes Verhalten der Agentsoftware fest. Das heißt, sie können auf Ressourcen zugreifen, die der hierarchiebasierten Benutzerkonfiguration zugeordnet sind, statt auf Ressourcen, die der gruppenbasierten Benutzerkonfiguration zugeordnet sind.
- Wenn Sie die Einstellungen in einer vorhandenen einer Hierarchie zugeordneten Benutzerkonfiguration erhalten, aber deren Zuordnung ändern möchten, verschieben Sie die Benutzerkonfiguration wie unter „So verschieben Sie eine Benutzerkonfiguration zu anderen Benutzern“ auf Seite 148 beschrieben. Diese Vorgehensweise gilt für hierarchiebasierte Benutzerkonfigurationen der Versionen 4.1, 4.5 und 4.6.

Hinweis: Wenn Sie den Password Manager-Dienst und die Password Manager Console, jedoch nicht die Agentsoftware aktualisieren, können Benutzer, deren Benutzerkonfigurationen mit Active Directory-Hierarchien (Organisationseinheiten oder Benutzer) verknüpft sind, dennoch die grundlegenden Funktionen der Agentsoftware verwenden. Jedoch haben die Benutzer dann keinen Zugriff auf die aktuellen Funktionen von Password Manager. Citrix empfiehlt, die Agentsoftware möglichst zu aktualisieren, damit sie mit den Versionen des Dienstes und der Konsole übereinstimmt.

Benutzerauthentifizierung und Identitätsprüfung

Password Manager stellt mehrere Authentifizierungsmethoden bereit, mit denen die Identität der Benutzer geprüft werden kann. In diesem Kapitel werden Strategien zur Entscheidungsfindung bei der Wahl der Authentifizierungsmethode beschrieben.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

Password Manager-Authentifizierung im Überblick

In Password Manager gibt es zwei Authentifizierungstypen:

- Primäre Authentifizierung: Diese Art der Authentifizierung erfolgt, wenn der Benutzer seine primären Zugangsdaten (Benutzername, Kennwort und optional Domänenname) im Windows-Anmeldedialogfeld eingibt, um auf das Unternehmensnetz zuzugreifen. Das vorhandene Windows-Sicherheitsteilsystem ist für die Verwaltung der Netzwerkauthentifizierung zuständig.
- Sekundäre Authentifizierung: Diese Art der Authentifizierung erfolgt, wenn Sie Password Manager zum Senden von Anmeldeinformationen konfigurieren, mit denen die Benutzer auf geschützte Ressourcen zugreifen können, für die die Single Sign-On-Funktion aktiviert ist. Diese Ressourcen sind beispielsweise Unternehmensanwendungen, Webanwendungen, geschützte Felder innerhalb von Anwendungen, IP-Adressen, URLs usw.

Nach der erfolgreichen Authentifizierung am Netzwerk bezieht Password Manager das primäre Kennwort und weitere Variablen über die Windows-Anmeldung und erstellt mit diesen Informationen den Verschlüsselungsschlüssel, der die Anmeldeinformationen geschützt. Die Agentsoftware ruft mit diesem Schlüssel die Anmeldeinformationen ab und entschlüsselt sie, wenn die Anmeldeinformationen von Anwendungen oder Ressourcen angefordert werden.

Wichtig: Wenn das Kennwort eines Benutzers kompromittiert ist, setzen Sie das Kennwort des Benutzers nicht nur einmal, sondern zweimal zurück, um sicherzustellen, dass das kompromittierte Kennwort nicht als altes Kennwort zur Identitätsprüfung verwendet wird. Benutzer müssen sich mit jedem der neuen Kennwörter anmelden, damit die Agentsoftware die Änderungen aufzeichnen kann.

Bestätigen der Benutzeridentität

Wenn sich Benutzer an der Umgebung anmelden, bestätigen sie die Identität durch die Eingabe des Benutzernamens und des Kennworts oder verwenden eine Smartcard oder ein anderes Authentifizierungsgerät zur eindeutigen Prüfung der Authentizität.

In verschiedenen Fällen wird jedoch eine zweite Stufe der Authentifizierung benötigt, um zu prüfen, dass der Benutzer, der die Änderung vornimmt, auch die entsprechenden Berechtigungen hat:

Ereignis	Beschreibung
Umgehen von Password Manager.	Wenn Benutzer das primäre Kennwort auf einem Gerät ändern, auf dem Password Manager installiert ist, und nicht Strg+Alt+Entf verwenden, kann Password Manager nicht bestätigen, dass der berechtigte Benutzer die Kennwortänderung ausgelöst hat.
Der Administrator ändert das Hauptkennwort eines Benutzers.	Wenn ein Administrator das primäre Kennwort eines Benutzers ändert, muss der Benutzer seine Identität bestätigen, um sicherzustellen, dass ein autorisierter Benutzer angemeldet ist.
Benutzer setzen das Hauptkennwort mit dem Konto-Self-Service zurück.	Wenn Benutzer das primäre Kennwort mit dem benutzerseitigen Zurücksetzen des Kennworts ändern, müssen sie auch die Identität bestätigen. Verwenden Sie nicht ausschließlich die Authentifizierung mit dem alten Kennwort im Zusammenhang mit der benutzerseitigen Kennwortzurücksetzung.
Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.	Wenn Benutzer die Sperrung des Kontos mit dem Konto-Self-Service aufheben, müssen sie die Identität erneut bestätigen.
Benutzer ändern den Authentifizierungstyp.	Wenn Benutzer beispielsweise von der Smartcard-Authentifizierung zur kennwortbasierten Authentifizierung wechseln, müssen sie ihre Identität erneut bestätigen.
Ändern des Kennworts auf einem Clientgerät ohne Password Manager.	Benutzer, die das primäre Kennwort auf einem Clientgerät ändern, auf dem die Agentsoftware nicht ausgeführt wird, werden bei der nächsten Anmeldung an einem Clientgerät, auf dem die Agentsoftware ausgeführt wird, zum Bestätigen der Identität aufgefordert.

Die Benutzer können die Identität mit den von Ihnen angegebenen Optionen (abhängig von den Unternehmensanforderungen) ändern. Weitere Informationen hierzu finden Sie unter „Methoden zur Identitätsprüfung im Überblick“ auf Seite 154.

Methoden zur Identitätsprüfung im Überblick

Für die unter „Bestätigen der Benutzeridentität“ auf Seite 153 beschriebenen Ereignisse stellt Password Manager zwei Methoden zur Identitätsprüfung zur Verfügung, mit denen sichergestellt werden kann, dass der Benutzer zur Verwendung von Password Manager berechtigt ist.

- „Altes Kennwort“ auf Seite 154
- „Sicherheitsfragen“ auf Seite 155

Wenn die Prüfung der Identität ausgelassen werden soll, können Sie die Funktion zur automatischen Schlüsselverwaltung verwenden. Weitere Informationen finden Sie unter „Auslassen der Identitätsprüfung“ auf Seite 156.

Unter „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132 werden die Benutzerkonfigurationsoptionen im Zusammenhang mit der Authentifizierung und der Identitätsprüfung beschrieben.

Hinweis: Sie können die Benutzer frei zwischen den Methoden für ihre Authentifizierung wählen lassen (altes Kennwort oder Sicherheitsfragen). Diese Option steht unter der Eigenschaft **Sekundäre Datenschutzmethode** in der Benutzerkonfiguration zur Verfügung.

Altes Kennwort

Bei Verwendung dieser Methode wird die Identität des Benutzers mit dem eingegebenen alten Kennwort geprüft.

Achtung: Wenn als Authentifizierungsmethode nur die Identitätsprüfung mit dem altem Kennwort zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, vom System ausgesperrt. Die Daten der Benutzer müssen aus dem zentralen Speicher und von allen Clientgeräten gelöscht werden, auf denen sie gespeichert sind. Die Benutzer müssen die Anmeldeinformationen für alle Anwendungen neu eingeben. Weitere Informationen finden Sie unter „Zurücksetzen und Löschen von Benutzerdaten“ auf Seite 141.

Sicherheitsfragen

Hinweis: Informationen zum Erstellen von Sicherheitsfragen finden Sie unter „Verwalten der fragenbasierten Authentifizierung“ auf Seite 159.

Wenn ein Benutzer sein primäres Kennwort ändert, können Sie die Identität des Benutzers bestätigen, indem der Benutzer die Sicherheitsfragen im Fragenkatalog beantwortet, den Sie erstellen. Dieser Fragenkatalog wird beim ersten Starten der Agentsoftware angezeigt. Benutzer beantworten die erforderliche Anzahl der Sicherheitsfragen und müssen diese Informationen bei bestimmten Kennwortänderungsereignissen erneut eingeben.

Die im Fragenkatalog enthaltenen Fragen sollten so abgefasst sein, dass nur die Person, die die Frage beantwortet, die Antwort kennt oder leicht erraten kann. Sie können die von Password Manager bereitgestellten Standardfragen verwenden oder eigene Fragen erstellen. Weitere Informationen finden Sie unter „Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit“ auf Seite 165.

Auslassen der Identitätsprüfung

Wichtig: Die automatische Schlüsselverwaltung ist nicht so sicher wie andere Methoden zur Schlüsselwiederherstellung, z. B. Sicherheitsfragen und altes Kennwort.

Wenn Password Manager die Prüfung der Identität auslassen und die Verschlüsselungsschlüssel der Benutzer automatisch abrufen soll, aktivieren Sie unter **Sekundäre Datenschutzmethode** die Option **Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt** (benötigt das Schlüsselverwaltungsmodul).

Diese Methode, die automatische Schlüsselverwaltung, steht zur Verfügung, wenn Sie das Modul **Schlüsselverwaltung** installieren und eine Benutzerkonfiguration erstellen, bei der diese Option aktiviert ist. Weitere Informationen finden Sie unter „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132.

Bei dieser Methode melden sich die Benutzer am Netzwerk an und können sofort auf Anwendungen zugreifen, die von Password Manager verwaltet werden. Es müssen keine Fragen beantwortet werden. Wenn ein Benutzer sein primäres Kennwort ändert, erkennt der Agent die Kennwortänderungen und stellt die Schlüssel des Benutzers mit dem Password Manager-Dienst wieder her.

Die automatische Schlüsselverwaltung ist für die Benutzer die einfachste und schnellste Methode zum Zugreifen auf die von ihnen genutzten Anwendungen. Allerdings schützt sie nicht vor unbefugtem Zugriff, da es kein nur dem Benutzer bekanntes „Geheimnis“ gibt, mit dem das Netzwerkkennwort des Benutzers geschützt wird. Um dieses potenzielle Problem zu verhindern, sollten Sie die automatische Schlüsselverwaltung zusammen mit dem Self-Service-Modul implementieren. Bei diesem Modul müssen die Benutzer ihre Identität mit einer fragenbasierten Authentifizierung bestätigen, wenn sie ihre primären Kennwörter zurücksetzen oder die Sperrung ihres Domänenkontos aufheben.

Benutzerseitiges Wechseln zwischen Authentifizierungsmethoden

In Citrix Password Manager können die Benutzer zwischen den verschiedenen Authentifizierungsmethoden wechseln. Password Manager schützt die Benutzerkennwörter mit einer eindeutigen Kopie des Sicherheitsschlüssels als Methode zur Neuauthentifizierung. Damit werden die Benutzerdaten jedes Mal, wenn der Benutzer zwischen den Authentifizierungsmethoden wechselt, freigegeben, ohne dass der Benutzer seine Identität bestätigen muss.

Die Option zur Auswahl verschiedener Authentifizierungsmethoden steht auf der Seite **Datenschutzmethode** in der Benutzerkonfiguration zur Verfügung. Weitere Informationen finden Sie unter „Planen der Benutzerkonfigurationen“ im *Citrix Password Manager-Installationshandbuch* und „Datenschutzmethoden auswählen“ auf Seite 129.

Beispiel:

- Ein Callcenter-Supervisor meldet sich mit seinen primären Anmeldeinformationen (Windows-Benutzername und -Kennwort) am PC an. Auf dem PC ist Password Manager Agent installiert, d. h. der Benutzer kann die Anwendungen verwenden, für die Single Sign-On aktiviert ist.
- Der Supervisor meldet sich gelegentlich mit einer Smartcard und PIN an einem gemeinsam genutzten PC im Callcenter an und startet eine weitere veröffentlichte Anwendung über den Presentation Server. Dieser PC verwendet Hotdesktop, um ein schnelles Wechseln zwischen verschiedenen Benutzern mit unterschiedlichen Konten zu ermöglichen.

In Version 4.0 und 4.1 von Password Manager muss der Callcenter-Supervisor vor der Verwendung von Single Sign-On-aktivierten Anwendungen seine Identität bei jedem Wechsel der primären Authentifizierungsmethoden bestätigen. In diesem Beispiel wurden zwei primäre Authentifizierungsmethoden verwendet: zuerst Benutzername und Kennwort, dann Smartcard mit PIN. In Version 4.0 und 4.1 von Password Manager ist beim Wechsel der Authentifizierungsmethode die Wiederherstellung des Sicherheitsschlüssels und möglicherweise die Bestätigung der Identität erforderlich.

Hinweis: Wenn ein Benutzer zum ersten Mal eine neue Authentifizierungsmethode verwendet oder zu einer neuen wechselt, muss diese Methode zuerst registriert werden. Wird diese neue Methode jedoch später wieder verwendet, muss sie nicht erneut registriert werden (d. h. danach ist keine Schlüsselwiederherstellung mehr notwendig).

Verwalten der fragenbasierten Authentifizierung

Wichtig: Wenn Sie die im Modul **Schlüsselverwaltung** von Password Manager enthaltenen Self-Service-Funktionen zur Kennwortzurücksetzung bzw. zum Aufheben der Sperrung des Domänenkontos verwenden möchten, müssen Sie die fragenbasierte Authentifizierung verwenden, damit Benutzer beim Zurücksetzen des primären Kennworts oder Aufheben der Sperrung des Domänenkontos ihre Identität bestätigen können.

Die fragenbasierte Authentifizierung bietet eine sichere Authentifizierung für Benutzer, die das primäre Kennwort in bestimmten Situationen bzw. die Authentifizierungsmethode ändern oder deren Konto gesperrt ist.

Die Verwendung von Sicherheitsfragen und fragenbasierter Authentifizierung kann den Zugriff nicht berechtigter Benutzer verhindern, da Informationen verlangt werden, die nur der Benutzer kennt. Sie sollten bei der Erstellung der Fragen darauf achten, dass nur Informationen abgefragt werden, die nicht öffentlich zugänglich sind und die nur der zu authentifizierende Benutzer wissen oder herausfinden kann. Auf diese Weise werden das Erraten der Antworten, Wörterbuchangriffe u. ä. die Sicherheit bedrohende Angriffe erschwert.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Bestätigen der Benutzeridentität durch die fragenbasierte Authentifizierung“ auf Seite 161
- „Arbeitsablauf zur fragenbasierten Authentifizierung“ auf Seite 163
- „Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit“ auf Seite 165
- „Verwalten der Fragen“ auf Seite 167
- „Rückwärtskompatibilität mit Password Manager Version 4.0 und 4.1“ auf Seite 179
- „Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen“ auf Seite 181

Bestätigen der Benutzeridentität durch die fragenbasierte Authentifizierung

Verwenden Sie die fragenbasierte Authentifizierung zur Prüfung der Benutzeridentität, wenn Sie die im Modul **Schlüsselverwaltung** von Password Manager verfügbaren Self-Service-Funktionen zur Kennwortzurücksetzung bzw. zum Aufheben der Sperrung des Domänenkontos implementieren. Sie können die fragenbasierte Authentifizierung auch als sekundären Datenschutz wählen, wenn sich die primäre Authentifizierung für einen Benutzer ändert. Weitere Informationen finden Sie unter „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132.

Je nach den Einstellungen in der Benutzerkonfiguration der Konsole kann es in folgenden Fällen erforderlich sein, die Identität der Benutzer zu prüfen:

- Der Benutzer ändert den Authentifizierungstyp, z. B. wenn zwischen der Authentifizierung mit Smartcard und mit Kennwort gewechselt wird.
- Der Administrator ändert das primäre Kennwort eines Benutzers.
- Benutzer setzen das Hauptkennwort mit dem Konto-Self-Service zurück.
- Benutzer heben die Sperrung des Domänenkontos mit dem Konto-Self-Service auf.
- Benutzer ändern das Hauptkennwort auf einem Computer, auf dem die Agentsoftware nicht installiert ist, und melden sich dann an einem Gerät an, auf dem die Agentsoftware installiert ist.

Hinweis: Sie können auch eine Benutzerkonfiguration erstellen, für die keine nachfolgende Prüfung beim Wechsel zwischen Authentifizierungstypen erforderlich ist. Weitere Informationen finden Sie unter „Benutzerseitiges Wechseln zwischen Authentifizierungsmethoden“ auf Seite 157.

Wenn Password Manager Agent konfiguriert ist, werden Benutzer beim ersten Verwenden von Password Manager Agent aufgefordert, die Sicherheitsfragen zu beantworten. Wenn ein Ereignis eintritt, für das eine Prüfung der Benutzeridentität erforderlich ist, startet der Agent den von Ihnen erstellten Fragenkatalog. Ein Fragenkatalog ist eine vorkonfigurierte Liste von Fragen, die Sie erstellen.

Jede Frage im Fragenkatalog wird auf einer einzelnen Seite angezeigt. Beispiel: Wenn der Fragenkatalog fünf Fragen enthält, werden den Benutzern fünf Seiten angezeigt, eine für jede Frage. Benutzer müssen jede Frage richtig beantworten. Abhängig von den Administratoreinstellungen müssen die Antworten genau mit den Antworten übereinstimmen (einschließlich der Groß- und Kleinschreibung), die Benutzer bei der Erstverwendung von Password Manager eingegeben haben.

Die richtige Kombination aus Fragen und Antworten bestätigt die Identität des Benutzers. Sobald eine Bestätigung erfolgt, verschlüsselt die Agentsoftware die Schlüssel mit dem neuen primären Kennwort und speichert die sekundären Anmeldeinformationen des Benutzers.

Überlegungen

Hinweis: Abhängig von den Einstellungen des Administrators sind die Groß- und Kleinschreibung, Satzzeichen und Leerzeichen in der Antwort des Benutzers enthalten und müssen genau übereinstimmen, wenn der Benutzer später zur Beantwortung der ausgewählten Sicherheitsfrage aufgefordert wird.

- Wenn Sie keine Antworten auf Sicherheitsfragen konfigurieren, werden Benutzer zur Eingabe des primären Kennworts aufgefordert, wenn sie das primäre Kennwort ändern und eine Anmeldung mit dem neuen Kennwort versuchen. Sie können die Benutzer frei zwischen den Methoden für ihre Authentifizierung wählen lassen. Diese Option ist als Teil der Eigenschaft **Sekundäre Datenschutzmethode** in der Benutzerkonfiguration verfügbar. Weitere Informationen finden Sie unter „Sekundäre Datenschutzoptionen auswählen“ auf Seite 132.
- Um zu vermeiden, dass Benutzer gesperrt werden, sollten Sie die benutzerseitige Kennwortrücksetzung nicht ausschließlich mit der Identitätsprüfung mit dem alten Kennwort kombinieren. Benutzer, die das Kennwort rücksetzen, können sich in der Regel nicht an das alte primäre Kennwort erinnern und sind damit nicht in der Lage, ihre sekundären Anmeldeinformationen abzurufen.
- Mehrere Fragen geben den besten Datenschutz. Weitere Informationen zur Erstellung von sicheren Fragen finden Sie unter „Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit“ auf Seite 165.
- In der Standardeinstellung werden für die fragenbasierte Authentifizierung vier Sicherheitsfragen verwendet. Sie können sich zwar auf diese vier Fragen beschränken, es wird jedoch empfohlen, eigene Sicherheitsfragen und Fragengruppen hinzuzufügen. Weitere Informationen finden Sie unter „Verwalten der Fragen“ auf Seite 167.

Arbeitsablauf zur fragenbasierten Authentifizierung

Wichtig: Erstellen Sie die Sicherheitsfragen und machen Sie die Fragen verfügbar, bevor Sie die Agentsoftware bereitstellen. Wenn ein Benutzer eine Frage ausgewählt hat, muss diese jederzeit zur Verfügung stehen. Wenn Sie eine Frage, die verwendet wird, ändern oder entfernen, können die Benutzer die sekundären Anmeldeinformationen erst mit der Sicherheitsfrage wiederherstellen, wenn sie sich erneut registriert haben. Weitere Informationen finden Sie unter „Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen“ auf Seite 144.

1. Erstellen Sie die Sicherheitsfragen, legen Sie die Mindestlänge und die Erkennung der Groß- und Kleinschreibung fest. Diese Fragen können in den Sprachen erstellt werden, die Password Manager unterstützt.
2. Sie können diese Fragen auch in Sicherheitsfragengruppen gruppieren. Sie können mehrere Fragen erstellen, unter denen die Benutzer auswählen können. Dies ermöglicht den Benutzern eine Frage auszuwählen, deren Antwort sie leichter behalten können. Sie können dann festlegen, wie viele Fragen von jeder Gruppe die Benutzer beantworten müssen.
3. Fügen Sie die Fragen oder Fragengruppen dem Fragenkatalog hinzu.
4. Wählen Sie maximal zwei Fragen aus, die für die Schlüsselwiederherstellung verwendet werden. Mit diesen Fragen werden die Daten für die Schlüsselwiederherstellung verschlüsselt. Die Benutzer müssen jedoch weiterhin die Fragen beantworten, die sie bei der Registrierung ausgewählt haben.

5. Sie können optional auch das Maskieren der Sicherheitsfragen aktivieren. Mit dieser Funktion können Sie die Benutzerantworten auf Sicherheitsfragen der fragenbasierten Authentifizierung maskieren. Wenn die Option aktiviert ist, sind die Antworten der Benutzer bei der Registrierung der Antworten und der Identitätsprüfung geschützt.

Wichtig: Wenn Sie das Maskieren der Sicherheitsfragen für bestehende Benutzer mit IMEs aktivieren, können die Benutzer möglicherweise keine Antworten bei der Registrierung und Identitätsprüfung eingeben. Ostasiatische Sprachen, wie Chinesisch, Japanisch und Koreanisch, benötigen einen IME für die Eingabe von Zeichen in der Password Manager-Benutzeroberfläche. Wenn Sie das Maskieren aktivieren, wird der IME automatisch bei der Registrierung und der Identitätsprüfung für die Benutzer deaktiviert, die auf Password Manager 4.6 aktualisiert haben.

Für neue Benutzer von Password Manager mit Version 4.6 besteht keine Auswirkung.

Hinweis: Das Maskieren der Antworten auf die Sicherheitsfragen steht nur in der Version der Konsole und der Agentsoftware zur Verfügung, die mit Password Manager 4.6 ausgeliefert wird.

Formulieren von Sicherheitsfragen: Sicherheit und Benutzerfreundlichkeit

Password Manager bietet vier Standardfragen, die Sie für die Benutzerregistrierung verwenden können. Diese Fragen stehen in allen unterstützten Sprachen (Deutsch, Englisch, Französisch, Japanisch und Spanisch) zur Verfügung. Citrix empfiehlt, dass Sie eigene Sicherheitsfragen erstellen und sie in jeder Sprache zur Verfügung stellen, die in der Umgebung unterstützt wird.

Ein Unbefugter, der versucht, das Kennwort eines Benutzers zu erfahren, muss die Antworten auf alle Fragen kennen, die der Benutzer anfänglich beantwortet hat. Berücksichtigen Sie jedoch, dass es für Benutzer sehr schwierig werden könnte, die Identitäten zu bestätigen, wenn sie zu viele Fragen beantworten müssen.

Sicherheitsfragen sollten nur Informationen abfragen, die nicht öffentlich zugänglich sind und die nur der autorisierte Benutzer wissen kann. Dies erschwert das Erraten der Antworten oder Wörterbuchangriffe. Der wichtigste Faktor bei der Ermittlung der Sicherheit einer Frage ist, wie schwierig es für andere Personen ist, die Antwort zu erraten.

Gute Fragen haben ein *hohes Maß* für den Informationsgehalt, also Fragen, für die Folgendes gilt:

- Die Anzahl der eindeutigen Antworten ist möglicherweise sehr hoch.
- Die Wahrscheinlichkeit, eine bestimmte Antwort zu raten, ist sehr niedrig.

Aus Verwendungsgründen sollte sich der Benutzer die Frage leicht merken können, die Frage sollte aber für einen Unbefugten schwer zu erraten sein. Beispiel:

- Wie lautet der Name Ihres Lieblingsprofessors oder Lieblingslehrers?
- Wo würden Sie für den ultimativen Traumurlaub hinfahren? (Stadt, Land)
- Wie lautet der Titel Ihres Lieblingsschlagers, oder wie heißt der Künstler?
- Wie lautet der Titel Ihres Lieblingsbuchs, wie heißt der Autor?
- Wie lautet der Name Ihres Lieblingskunstwerks, des Künstlers, wo ist das Kunstwerk ausgestellt?

Bei diesen weiteren Beispielen kann es jedoch passieren, dass Benutzer mit demselben sozialen Hintergrund identische Antworten auf diese Fragen geben, auch wenn sie ihre Antworten gar nicht weitergegeben haben. Dies erhöht das Risiko von Insiderangriffen.

Vermeiden Sie das Erstellen von Fragen, die folgende Merkmale aufweisen:

- Einfache Antworten, z. B. Lieblingsfarbe
- Bekannte oder sich ändernde Informationen, z. B. Adresse

Überlegungen zu Sicherheitsfragen

- Wenn Sie die bestehenden Standardfragen ändern, nachdem Benutzer die Antworten gespeichert haben, sollten Sie die Bedeutung der bearbeiteten Fragen berücksichtigen. Wenn Sie eine Frage bearbeiten, müssen sich die Benutzer nicht neu registrieren. Wenn Sie jedoch die Bedeutung der Frage ändern, könnten Benutzer, die diese Frage beantwortet haben, möglicherweise nicht die richtige Antwort eingeben.
- Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Agentsoftware starten.
- Einzelne Sicherheitsfragen können zu mehreren Sicherheitsfragengruppen gehören. Wenn Sie Sicherheitsfragengruppen erstellen, können alle erstellten Fragen in jeder Sicherheitsfragengruppe verwendet werden.

Verwalten der Fragen

Der Knoten **Fragenbasierte Authentifizierung** in der Password Manager Console bietet einen zentralen Speicherort für die Verwaltung aller Sicherheitsfragen, die mit der Identitätsprüfung, der benutzerseitigen Kennwortzurücksetzung und dem Aufheben der Kontosperrung verbunden sind. Sie können der Liste der Standardfragen eigene Sicherheitsfragen hinzufügen sowie Fragengruppen erstellen und diese für bestimmte Benutzer verwenden.

In diesem Abschnitt wird Folgendes beschrieben:

- „Einstellen der Standardsprache“ auf Seite 168
- „Erstellen neuer Sicherheitsfragen“ auf Seite 169
- „Hinzufügen oder Bearbeiten von Text für bestehende Fragen (einschließlich Textübersetzungen)“ auf Seite 170
- „Erstellen von Sicherheitsfragengruppen“ auf Seite 172
- „Erstellen und Implementieren des Fragenkatalogs“ auf Seite 174
- „Auswählen von Fragen für die Schlüsselwiederherstellung“ auf Seite 176
- „Aktivieren des Maskierens der Antworten auf Sicherheitsfragen“ auf Seite 177

Siehe auch:

- „Rückwärtskompatibilität mit Password Manager Version 4.0 und 4.1“ auf Seite 179
- „Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen“ auf Seite 181

Einstellen der Standardsprache

Den Benutzern werden die Sicherheitsfragen meistens in der Sprache angezeigt, die dem aktuellen Benutzerprofil zugeordnet ist. Wenn die Sprache nicht zur Verfügung steht, zeigt Password Manager die Fragen in der von Ihnen gewählten Standardsprache an.

So stellen Sie die Standardsprache ein

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie die Knoten **Password Manager** und **Identitätsprüfung** und wählen Sie in der Password Manager Console **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Das Dialogfeld **Fragen verwalten** wird angezeigt.
4. Wählen Sie **Fragenbasierte Authentifizierung** aus.
5. Wählen Sie aus der Dropdownliste **Sprache** die Standardsprache aus.
6. Klicken Sie auf **OK**.

Hinweis: Wenn in diesem Dialogfeld die Option **Prüfung auf Rückwärtskompatibilität durchführen** ausgewählt ist, wird sichergestellt, dass die Fragen zur Identitätsprüfung in den Versionen 4.0 und 4.1 von Password Manager Agent weiterhin angezeigt werden können. Weitere Informationen finden Sie unter „Rückwärtskompatibilität mit Password Manager Version 4.0 und 4.1“ auf Seite 179.

Erstellen neuer Sicherheitsfragen

Sie können beliebig viele Fragen erstellen und jeder Frage eine Sprache zuweisen. Sie können auch mehrere Übersetzungen einer Frage bereitstellen. Die Agentsoftware zeigt dem Benutzer den Fragenkatalog in der Sprache an, die den Spracheinstellungen des Benutzerprofils entspricht. Wenn die Sprache nicht zur Verfügung steht, zeigt Password Manager die Fragen in der Standardsprache an.

So erstellen Sie neue Sicherheitsfragen

Hinweis: In der Standardeinstellung wird als Sprache Englisch angezeigt. Wenn Sie die Sprache für eine Sicherheitsfrage angeben, wird die Frage den Benutzern angezeigt, deren Betriebssystemeinstellungen für diese Sprache konfiguriert sind. Wenn die ausgewählten Einstellungen des Betriebssystems nicht mit den verfügbaren Fragen übereinstimmt, wird den Benutzern die ausgewählte Standardsprache angezeigt.

---

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Sicherheitsfragen** aus.
5. Wählen Sie in der Dropdownliste **Sprache** eine Sprache aus und klicken Sie auf **Frage hinzufügen**.

   Der Editor für **Sicherheitsfragen**wird angezeigt.

6. Führen Sie im Editor folgende Aktionen aus:
   A. Geben Sie im Textfeld **Sicherheitsfrage** eine neue Frage ein.
   B. Wählen Sie die Mindestlänge der erforderlichen Antwort aus.
   C. Aktivieren Sie **Bei Antwort wird Groß-/Kleinschreibung erkannt**, wenn die Antwort darauf überprüft werden soll. Deaktivieren Sie dieses Kontrollkästchen, wenn die Groß-/Kleinschreibung der Antwort nicht berücksichtigt werden soll.
7. Klicken Sie auf **OK**, um die Frage und Einstellungen zu speichern.
8. Klicken Sie auf **OK**, um das Dialogfeld **Fragen verwalten** zu schließen.

Wichtig: Sie müssen den übersetzten Text bestehender Fragen mit dem Befehl **Bearbeiten** hinzufügen. Wenn Sie **Hinzufügen** auswählen, erstellen Sie eine neue Frage, die nicht mit der Originalfrage verknüpft ist.

Hinzufügen oder Bearbeiten von Text für bestehende Fragen (einschließlich Textübersetzungen)

Wichtig: Wenn Sie Sicherheitsfragen hinzufügen, löschen und ersetzen, nachdem sich Benutzer registriert haben, müssen sich alle Benutzer, die sich mit den alten Fragen registriert haben, neu registrieren, um sich zu authentifizieren und das Kennwort zurückzusetzen. Benutzer müssen die neuen Fragen beantworten, wenn sie die Agentsoftware starten. Wenn Sie eine Frage bearbeiten, müssen sich die Benutzer nicht neu registrieren. Wenn Sie jedoch die Bedeutung der Frage ändern, können Benutzer, die diese Frage beantwortet haben, möglicherweise nicht die richtige Antwort eingeben.

So fügen Sie Text für bestehende Fragen hinzufügen oder bearbeiten den Text

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.

3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren

4. Wählen Sie **Sicherheitsfragen** aus.
5. Wählen Sie eine Sprache aus der Dropdownliste **Sprache** aus.
6. Wählen Sie die Frage aus und klicken Sie auf **Bearbeiten**.

   Wichtig: Wenn Sie eine bestehende Frage bearbeiten, wird in einer Warnmeldung darauf hingewiesen, dass ein Ändern der Bedeutung einer Frage zu nicht übereinstimmenden Benutzerantworten bei der Neuauthentifizierung führen kann. Ein Benutzer könnte also eine andere Antwort eingeben, die nicht mit der gespeicherten Antwort übereinstimmt.

   Der Editor für **Sicherheitsfragen**wird angezeigt.

7. Führen Sie folgende Aktionen im Editor aus:

   A. Geben Sie im Textfeld **Sicherheitsfrage** eine Frage ein oder bearbeiten Sie die Frage.

   B. Wählen Sie die Mindestlänge der erforderlichen Antwort aus.

   C. Aktivieren Sie **Bei Antwort wird Groß-/Kleinschreibung erkannt**, wenn die Antwort darauf überprüft werden soll. Deaktivieren Sie dieses Kontrollkästchen, wenn die Groß-/Kleinschreibung der Antwort nicht berücksichtigt werden soll.

8. Klicken Sie auf **OK**, um die Frage und Einstellungen zu speichern.
9. Wiederholen Sie die Schritte 5 bis 8 für jede Frage und Sprache.
10. Klicken Sie auf **OK**, um das Dialogfeld **Fragen verwalten** zu schließen.

Erstellen von Sicherheitsfragengruppen

Sie können mehrere Sicherheitsfragen erstellen, die Benutzer beantworten, um die Identität zu bestätigen. Jede Frage, die Sie dem Fragenkatalog hinzufügen, muss von den Benutzern beantwortet werden. Sie können die Fragen auch in einer *Sicherheitsfragengruppe* zusammenfassen.

Wenn Sie beispielsweise die Fragen in einer Gruppe zusammenfassen, können Sie dem Fragenkatalog sechs Fragen hinzufügen und Benutzer können z. B. drei der sechs Fragen im Fragenkatalog beantworten. Dies gibt Benutzern mehr Flexibilität bei der Auswahl und Beantwortung von Fragen für die Identitätsprüfung.

So erstellen Sie eine Sicherheitsfragengruppe

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Sicherheitsfragen** aus.
5. Klicken auf **Gruppe hinzufügen**

   Das Dialogfeld **Sicherheitsfragengruppe** wird mit einer Liste von verfügbaren Sicherheitsfragen für die Gruppe angezeigt.

6. Führen Sie folgende Aktionen im Dialogfeld aus:
   A. Geben Sie einen Namen für die Sicherheitsfragengruppe ein. Sie können ein Benennungsschema zur Identifizierung der Gruppen verwenden. Sie können z. B. den Fragen eine Beschreibung hinzufügen, wie z. B. „Filmgruppe“ oder „Hobbygruppe“.
   B. Aktivieren Sie das Optionsfeld neben jeder Frage, die Sie der Gruppe hinzufügen möchten.
   C. Wählen Sie die Anzahl der Fragen aus dieser Gruppe aus, die ein Benutzer beantworten muss.
7. Klicken Sie auf **OK**, um die Gruppe und Einstellungen zu speichern.
8. Wiederholen Sie die Schritte 5 bis 7, um weitere Gruppen zu erstellen.
9. Klicken Sie auf **OK**, um das Dialogfeld **Fragen verwalten** zu schließen.

So bearbeiten Sie eine Sicherheitsfragengruppe

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Sicherheitsfragen** aus.

5. Wählen Sie die Sicherheitsfragengruppe aus, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.

   Das Dialogfeld **Sicherheitsfragengruppe** wird mit einer Liste von verfügbaren Sicherheitsfragen für die Gruppe angezeigt. Die Fragen, die bereits in der Gruppe eingeschlossen sind, haben ein Häkchen. In diesem Dialogfeld können Sie den Namen der Gruppe bearbeiten, der Gruppe Fragen hinzufügen und die Anzahl der Fragen von dieser Gruppe auswählen, die der Benutzer beantworten muss.
6. Klicken Sie auf **OK**, um die Gruppe und Einstellungen zu speichern.
7. Klicken Sie auf **OK**, um das Dialogfeld **Fragen verwalten** zu schließen.

Erstellen und Implementieren des Fragenkatalogs

Die Benutzer sehen und beantworten die Sicherheitsfragen, die Sie als Fragenkatalog ausgewählt haben. Im Fragenkatalog sind Fragen und Fragengruppen zusammengestellt, die Sie erstellt und den Benutzern zur Verfügung gestellt haben.

Ein Fragenkatalog besteht aus einer Liste von Fragen und Fragengruppen. Sie können eine Frage nicht im Fragenkatalog wiederholen. Beispiel: Sie können keine Fragengruppe erstellen, die eine Frage enthält, die bereits im Fragenkatalog enthalten ist.

Einführung

- Einzelne Sicherheitsfragen können zu mehreren Sicherheitsfragengruppen gehören. Wenn Sie Sicherheitsfragengruppen erstellen, können alle erstellten Fragen in jeder Sicherheitsfragengruppe eingeschlossen werden.
- Wenn Sie ein Upgrade von einer vorherigen Password Manager-Version durchführen, müssen Sie möglicherweise Fragen und Fragengruppen mit bestimmten Einstellungen für die Rückwärtskompatibilität mit vorherigen Versionen der Password Manager Agent-Software hinzufügen.

So können Sie die Reihenfolge der Sicherheitsfragen im Fragenkatalog hinzufügen, entfernen oder ändern

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie die Option **Fragenkatalog** und klicken Sie auf **Hinzufügen**.
5. Wählen Sie die Sicherheitsfragen oder Sicherheitsfragengruppen aus, die Sie dem Fragenkatalog hinzufügen möchten.

   Wenn die Fragengruppe, die Sie hinzufügen, mehr Fragen enthält, als Benutzer beantworten müssen (z. B. drei von sechs Fragen), wählen Benutzer die Fragen in einem Listenfeld aus und geben die Antworten ein, bis die gewünschte Anzahl der Fragen beantwortet ist.
6. Sie können auf **Auf** oder **Ab** klicken, um die Reihenfolge zu ändern, in der die Fragen oder Fragengruppen den Benutzern angezeigt werden.
7. Sie können auch eine Frage auswählen und auf die Schaltfläche **Entfernen** klicken, um die Frage aus dem Fragenkatalog zu löschen.

   Hinweis: Wenn Sie eine Frage aus dem Fragenkatalog entfernen, wird sie bestehenden Benutzern zwar weiterhin angezeigt, sie wird jedoch nicht in die Liste der Fragen eingeschlossen, die neuen Benutzern angezeigt werden.

   ---
8. Klicken Sie auf **OK**, um den Fragenkatalog zu speichern.

   Möglicherweise werden Sie in einer Meldung aufgefordert festzulegen, ob Benutzer ihre Antworten stets neu registrieren sollen. Klicken Sie auf **Ja**, um die Registrierung zu erzwingen.

Auswählen von Fragen für die Schlüsselwiederherstellung

Sie müssen eine Frage oder zwei der Fragen auswählen, die Benutzer beantworten, um die Daten für die Schlüsselwiederherstellung zu verschlüsseln. Die Benutzer müssen die Antworten für alle Fragen eingeben, die sie bei der Registrierung beantwortet haben, mit den von Ihnen ausgewählten Fragen werden Daten bereitgestellt, die bei der Verschlüsselung und der Schlüsselwiederherstellung eingeschlossen werden.

So wählen Sie eine oder mehrere Fragen für die Schlüsselwiederherstellung aus

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Schlüsselwiederherstellung** aus.
5. Aktivieren Sie das Optionsfeld neben jeder Frage oder Fragengruppe, die Sie bei der Identitätsprüfung für die Schlüsselwiederherstellung verwenden möchten.
6. Klicken Sie auf **OK**, um die Frage und Einstellungen zu speichern.

   Möglicherweise werden Sie in einer Meldung aufgefordert festzulegen, ob Benutzer ihre Antworten stets neu registrieren sollen. Klicken Sie auf **Ja**, um die Registrierung zu erzwingen.

Aktivieren des Maskierens der Antworten auf Sicherheitsfragen

Hinweis: Das Maskieren der Antworten auf Sicherheitsfragen steht nur in Password Manager 4.6 zur Verfügung.

Wichtig: Wenn Sie das Maskieren der Antworten auf Sicherheitsfragen für bestehende Benutzer mit IMEs aktivieren, können die Benutzer möglicherweise keine Antworten bei der Registrierung und Identitätsprüfung eingeben. Ostasiatische Sprachen, wie Chinesisch, Japanisch und Koreanisch, benötigen einen IME für die Eingabe von Zeichen in der Password Manager-Benutzeroberfläche. Wenn Sie das Maskieren aktivieren, wird der IME automatisch bei der Registrierung und der Identitätsprüfung für die Benutzer deaktiviert, die auf Password Manager 4.6 aktualisiert haben.

Für neue Benutzer von Password Manager mit Version 4.6 besteht keine Auswirkung.

Das Maskieren der Antworten auf die Sicherheitsfragen gibt ein zusätzliches Sicherheitsniveau für die Benutzer, wenn sie die Antworten auf die Sicherheitsfragen registrieren oder die Antworten bei der Identitätsprüfung eingeben. Wenn diese Funktion aktiviert ist, sind die Antworten der Benutzer ausgeblendet, die Password Manager 4.6 ausführen. Bei der Registrierung der Antworten werden die Benutzer aufgefordert, die Antworten zweimal einzugeben, um Schreib- oder Rechtschreibefehler zu vermeiden. Benutzer müssen die Antworten bei der Identitätsprüfung nur einmal eingeben, da sie zur erneuten Eingabe aufgefordert werden, wenn Fehler bestehen.

Hinweis: Antworten auf Sicherheitsfragen, die in Password Manager Agent 4.5 registriert wurden, können maskiert werden, wenn Sie die Software auf Version 4.6 aktualisieren.

Antworten auf Sicherheitsfragen für Benutzer, die die Agentsoftware für Password Manager 4.5, 4.1 oder 4.0 verwenden, bleiben unabhängig von der Konsoleneinstellung sichtbar.

So aktivieren Sie das Maskieren der Antworten auf Sicherheitsfragen

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Antworten auf Sicherheitsfragen maskieren**.
5. Wählen Sie **Antworten auf Sicherheitsfragen maskieren**.
6. Klicken Sie auf **OK**, um die Einstellung zu speichern.

Rückwärtskompatibilität mit Password Manager Version 4.0 und 4.1

Mit dem Rückwärtskompatibilitätsmodus kann die Agentsoftware Benutzern Fragen zur Identitätsprüfung anzeigen, die Sie in den Password Manager-Versionen 4.0 und 4.1 verwendet haben. Im Rückwärtskompatibilitätsmodus können Sie auch weiterhin die Standardfrage „Wie lautet Ihr Satz zur Identitätsprüfung?“ verwenden. Wenn Sie ein Upgrade von Password Manager 4.1 durchführen, werden die Fragen zur Identitätsprüfung und die Fragen, die Sie für die benutzerseitige Kennwortrücksetzung verwendet haben, als Fragenkatalog im Editor **Fragen verwalten** angezeigt.

Wichtig: Wenn Sie Benutzerkonfigurationen erstellen und bearbeiten, sollten Sie die Rückwärtskompatibilität nicht aktivieren, wenn Sie eine neue Installation von Password Manager verwenden, da die Funktionalität der Agentsoftware auf die der Produktversion 4.0 und 4.1 eingeschränkt wird. Auch sollten Sie die Rückwärtskompatibilität nicht deaktivieren, wenn Sie die Agentsoftware von Version 4.0 oder 4.1 von Password Manager ausführen, da Sie dann die Schlüsselwiederherstellung und Registrierungen für die benutzerseitige Kennwortrücksetzung verhindern.

Aktivieren Sie die Rückwärtskompatibilität nicht, wenn Sie die automatische Schlüsselverwaltung verwenden. Für die automatische Schlüsselwiederherstellung müssen Benutzer keine Fragen zur Identitätsprüfung beantworten.

So aktivieren Sie die Rückwärtskompatibilität für den Fragenkatalog

Für die Rückwärtskompatibilität für Password Manager 4.0 und 4.1 muss der Fragenkatalog mindestens eine Sicherheitsfrage enthalten, die der Funktion zur benutzerseitigen Kennwortrücksetzung zugeordnet ist.

Jede Sicherheitsfrage muss die folgenden Einstellungen enthalten:

- Deaktivierte Erkennung der Groß- und Kleinschreibung
- Mindestlänge der Antwort ist 1
- Fragen können nicht für die Schlüsselwiederherstellung aktiviert sein

So prüfen Sie auf Rückwärtskompatibilität

Sie können die Rückwärtskompatibilität prüfen, wenn Sie von einer vorherigen Password Manager-Version aktualisieren:

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie den Knoten **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie im Bereich **Häufige Tasks** auf **Fragen verwalten**.

   Im angezeigten Dialogfeld **Fragen verwalten** sind vier Tasks verfügbar:

   - Fragenbasierte Authentifizierung
   - Sicherheitsfragen
   - Fragenkatalog
   - Schlüsselwiederherstellung
   - Antworten auf Sicherheitsfragen maskieren
4. Wählen Sie **Fragenbasierte Authentifizierung** aus.
5. Wählen Sie **Prüfung auf Rückwärtskompatibilität durchführen** aus und klicken Sie auf **OK**.

Password Manager führt die Prüfung auf Rückwärtskompatibilität aus und zeigt Fehler in einem Dialogfeld an.

Benutzerseitiges Neuregistrieren der Antworten auf die Sicherheitsfragen

Mit Password Manager können Benutzer Antworten auf die Sicherheitsfragen jederzeit und ohne Hilfe des Administrators neu registrieren.

Wenn Sie Sicherheitsfragen oder die Konto-Self-Service-Funktionen in der Umgebung verwenden, können Benutzer, die Sicherheitsfragen und Antworten registrieren, mit der Agentsoftware neue Antworten auf die verfügbaren Sicherheitsfragen eingeben.

Benutzer klicken im Anmeldungsmanager im Menü **Extras** auf **Sicherheitsfragenregistrierung** oder wählen den Eintrag im Kontextmenü des Infosymbols der Agentsoftware aus. Bei Auswahl dieser Option wird der Assistent für die Sicherheitsfragenregistrierung gestartet, mit dem Benutzer Antworten auf die Sicherheitsfragen neu registrieren können. Nach der erfolgreichen Eingabe der Antworten werden die Benutzer informiert, dass die neuen Antworten im zentralen Speicher gespeichert sind. Die alten Antworten sind nicht mehr gültig.

Diese Funktion steht nur für Benutzer bereit, die mit der aktuellen Version der Agentsoftware eine Verbindung mit Password Manager herstellen und die vorher Antworten auf die Sicherheitsfragen registriert haben.

Benutzerseitiges Verwalten der primären Anmeldeinformationen mit dem Konto-Self-Service

Sie können in den Self-Service-Funktionen von Password Manager konfigurieren, dass Benutzer ohne Beteilung des Administrators oder des Helpdeskpersonals das primäre Kennwort zurücksetzen oder die Sperrung der Windows-Domänenkonten aufheben können. Je nach Bedarf können Sie eine oder beide Konto-Self-Service-Funktionen (Kennwort zurücksetzen und Kontosperrung aufheben) sicher in der Password Manager-Umgebung implementieren.

In diesem Abschnitt werden die folgenden Themen beschrieben:

Hinweis: Weitere Informationen zur Implementierung des Konto-Self-Service mit dem Citrix Webinterface finden Sie im Webinterface-Administratorhandbuch auf der Citrix Website unter http://support.citrix.com.

Konto-Self-Service im Überblick

Die Konto-Self-Service-Funktionen werden durch die fragenbasierte Authentifizierung geschützt, die sicherstellt, dass Benutzer die Kennwörter zurücksetzen oder die Kontosperrung aufheben können. Wenn Benutzer Password Manager Agent das erste Mal oder das erste Mal nach der Konfiguration des Self-Service-Dienstes verwenden, müssen sie Antworten auf Sicherheitsfragen registrieren, die Sie bei der Einrichtung von Password Manager erstellen und auswählen.

Diese Sicherheitsfragen werden den Benutzern angezeigt, wenn sie das Kennwort zurücksetzen oder die Sperrung des Kontos aufheben möchten. Wenn die Fragen richtig beantwortet werden, können Benutzer ohne Beteiligung des Administrators oder Helpdeskpersonals das Kennwort zurücksetzen oder die Kontosperrung aufheben. Informationen zur fragenbasierten Authentifizierung finden Sie unter „Verwalten der fragenbasierten Authentifizierung“ auf Seite 159.

Wichtig: Fur die Self-Service-Funktionen zum Zurücksetzen des Kennworts und Aufheben der Kontosperrung ist die Implementierung der fragenbasierten Authentifizierung erforderlich. Um die Funktionen verwenden zu können, müssen Benutzer Antworten auf Sicherheitsfragen registrieren. Wenn die fragenbasierte Authentifizierung nicht in der Password Manager-Umgebung implementiert ist, stehen die Funktionen zum Zurücksetzen des Kennworts und Aufheben der Kontosperrung nicht zur Verfügung.

Überlegungen

- Sie können die Funktionen des Self-Service-Moduls, mit denen Benutzer das primäre Kennwort (für das Domänenkonto) zurücksetzen oder die Sperrung der Windows-Domänenkonten aufheben können, nur in einer Active Directory-Umgebung implementieren.
- Wenn Benutzer das Anwendungskennwort mit Password Manager Agent oder das primäre Kennwort mit der Tastenkombination STRG+ALT+ENTF auf einem Gerät ändern, auf dem die Agentsoftware installiert ist, erfasst Password Manager automatisch die Kennwortänderung.
- Um zu vermeiden, dass Benutzer ausgesperrt werden, sollten Sie die Self-Service-Funktion zum Zurücksetzen des Kennworts nicht ausschließlich mit der Identitätsprüfung mit dem alten Kennwort kombinieren. Wenn als Authentifizierungsmethode nur die Identitätsprüfung mit dem altem Kennwort zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, vom System ausgesperrt. Die Daten der Benutzer müssen aus dem zentralen Speicher und von allen Clientgeräten, auf denen sie gespeichert sind, gelöscht bzw. zurückgesetzt werden. Die Benutzer müssen die Anmeldeinformationen für alle Anwendungen neu eingeben. Weitere Informationen finden Sie unter „Zurücksetzen und Löschen von Benutzerdaten“ auf Seite 141.

Verwenden der automatischen Schlüsselverwaltung mit dem Konto-Self-Service

Wenn Sie den Konto-Self-Service mit der automatischen Schlüsselverwaltung kombinieren, vereinfacht dies die Arbeit für Benutzer, die auf kennwortgeschützte Anwendungen zugreifen müssen, die von der Password Manager Agent-Software verwaltet werden. So müssen Benutzer z. B. nach dem erfolgreichen Zurücksetzen der primären Kennwörter keine Sicherheitsfragen beantworten. (Die Sicherheitsfragen müssen allerdings beim Zurücksetzen der Kennwörter beantwortet werden.)

Bei der automatischen Schlüsselverwaltung wird die Identität der Benutzer nach dem Aufheben der Kontosperrung bzw. Zurücksetzen der Domänenpasswörter nicht geprüft.

Weitere Informationen finden Sie unter „Benutzererfahrung“ auf Seite 187.

Zusammenfassung der Implementierungsaufgaben für den Konto-Self-Service

Führen Sie für die Verwendung des Konto-Self-Service die folgenden Schritte aus:

Aufgabe	Siehe Abschnitt
Installieren Sie das Self-Service-Modul von Password Manager. Installieren Sie das Modul **Schlüsselverwaltung**.	„Installieren und Konfigurieren des Password Manager-Dienstes" im *Citrix Password Manager-Installationshandbuch*.
Konfigurieren Sie die fragenbasierte Authentifizierung.	„Verwalten der fragenbasierten Authentifizierung" auf Seite 159
Erstellen Sie eine Benutzerkonfiguration, in der eine oder beide der Self-Service-Funktionen (Kennwort zurücksetzen und Kontosperrung aufheben) aktiviert sind.	„Self-Service-Funktionen aktivieren" auf Seite 133
Installieren und konfigurieren Sie die Agentsoftware.	„Installieren und Konfigurieren von Password Manager Agent" im *Citrix Password Manager-Installationshandbuch*.

Benutzerseitiges Vergessen der Sicherheitsfragen

Wenn Benutzer die Antworten auf die Sicherheitsfragen vergessen, müssen Sie in der Password Manager Console die benutzerseitige Registrierung für den Self-Service zurücksetzen. Nach dem Zurücksetzen eines Benutzers oder aller Benutzer wird der Assistent für die Self-Service-Registrierung angezeigt, wenn Benutzer die Agentsoftware das nächste Mal öffnen. Die Benutzer können dann die Antworten auf die Sicherheitsfragen registrieren.

So setzen Sie die Registrierung des Benutzers für den Konto-Self-Service zurück

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und anschließend den Knoten **Identitätsprüfung** und wählen Sie **Fragenbasierte Authentifizierung** aus.
3. Klicken Sie unter **Häufige Tasks** auf **Die Registrierung der Sicherheitsfragen für einen Benutzer aufheben**.
4. Geben Sie im Dialogfeld **Benutzer auswählen** den Namen des Benutzers bzw. der Benutzergruppe ein und klicken Sie auf **OK**.
5. Bestätigen Sie die gewünschte Aufhebung der Registrierung für den ausgewählten Benutzer.

Benutzererfahrung

Nach der Installation und Konfiguration des Dienstes und der Agentsoftware fügt das Self-Service-Modul dem Windows-Anmeldedialogfeld des Benutzers und dem Dialogfeld **Sperrung des Computers aufheben** oder dem Dialogfeld **Willkommen bei Windows Vista** (das beim Drücken von STRG-ALT-ENTF zum Aufheben der Sperrung des Computers angezeigt wird) die Schaltfläche **Konto-Self-Service** hinzu.

Bevor die Benutzer auf die Self-Service-Funktionen zugreifen können, müssen sie sich an dem primären Domänenkonto anmelden und Antworten auf Sicherheitsfragen registrieren. Nach der erfolgreichen Registrierung können sie die Self-Service-Funktionen zum Zurücksetzen des Kennworts und Aufheben der Kontosperrung verwenden.

Wie unter „Verwenden der automatischen Schlüsselverwaltung mit dem Konto-Self-Service“ auf Seite 185 beschrieben, muss die Identität der Benutzer bei der automatischen Schlüsselverwaltung nach dem Aufheben der Kontosperrung bzw. Zurücksetzen der Domänenkennwörter nicht geprüft werden.

In der folgenden Tabelle wird die Benutzererfahrung bei Verwendung dieser Funktionen aufgeführt:

Ohne automatische Schlüsselverwaltung	**Mit automatischer Schlüsselverwaltung**
Der Benutzer klickt auf die Schaltfläche **Konto-Self-Service**.	Der Benutzer klickt auf die Schaltfläche **Konto-Self-Service**.
Der Benutzer wählt **Kontosperrung aufheben** oder **Kennwort zurücksetzen** aus.	Der Benutzer wählt **Kontosperrung aufheben** oder **Kennwort zurücksetzen** aus.
Der Benutzer beantwortet die Sicherheitsfragen richtig.	Der Benutzer beantwortet die Sicherheitsfragen richtig.
Der Benutzer gibt ein neues Kennwort ein und bestätigt es, klickt auf **Fertig stellen** und wird abgemeldet.	Der Benutzer gibt ein neues Kennwort ein und bestätigt es, klickt auf **Fertig stellen** und wird abgemeldet.
Der Benutzer meldet sich mit dem neuen Kennwort an und die Agentsoftware wird mit dem zentralen Speicher synchronisiert.	Der Benutzer meldet sich mit dem neuen Kennwort an und die Agentsoftware wird mit dem zentralen Speicher synchronisiert.
Je nach Einstellungen in der Benutzerkonfiguration stellt der Benutzer für die Identitätsprüfung nach der Kennwortänderung ein altes Kennwort bereit oder beantwortet Sicherheitsfragen. Bei einer richtigen Antwort kann der Benutzer auf die in Password Manager konfigurierten Single Sign-On-aktivierten Anmeldungen zugreifen. Informationen darüber, wie Sie vermeiden können, dass Benutzer ausgesperrt werden, finden Sie unter „Überlegungen“ auf Seite 185.	Eine Identitätsprüfung ist nicht erforderlich. Der Benutzer kann auf die in Password Manager konfigurierten Single Sign-On-aktivierten Anwendungen zugreifen.

Automatisieren der Eingabe der Anmeldeinformationen mit dem Provisioning

Hinweis: Mit dem Provisioningdienst können Sie die Anmeldeinformationen des Benutzers zurücksetzen und mehrere Benutzer und deren Anmeldeinformationen für Anwendungen in Password Manager löschen. Weitere Informationen zum Ausführen des Tasks für einen Benutzer finden Sie unter „Zurücksetzen und Löschen von Benutzerdaten“ auf Seite 141.

Die Agentsoftware verarbeitet jeden Befehl zum Zurücksetzen, wenn der Agent startet oder neu gestartet wird (wenn das Programm aktuell auf dem PC des Benutzers ausgeführt wird). Sonst verarbeitet die Agentsoftware alle anderen Provisioningbefehle, wenn der Agent gestartet oder neu gestartet wird, wenn der Benutzer im Anmeldungsmanager der Agentsoftware auf **Aktualisieren** klickt, oder wenn der Benutzer im Kontextmenü des Agentsymbols auf **Aktualisieren** klickt. Wenn die Warteschlange einen Befehl **Zurücksetzen** enthält, und der Benutzer auf **Aktualisieren** klickt, wird dem Benutzer in einer Meldung angezeigt, dass die Benutzerdaten zurückgesetzt wurden und ein Neustart von Password Manager Agent erforderlich ist.

In diesem Abschnitt wird beschrieben, wie Sie mit dem Provisioningdienst (auch als *Provisioning der Anmeldeinformationen* bezeichnet) Anmeldeinformationen des Benutzers manipulieren, die Anwendungen zugeordnet sind, die in einer Benutzerkonfiguration festgelegt sind. Mit dem Provisioning können Sie diese Tasks automatisieren und sie auf mehrere Benutzer anwenden. Beispielsweise können Sie mit dem Provisioning der Anmeldeinformationen verhindern, dass Benutzer bei der Erstverwendung der Agentsoftware die Ersteinrichtung der Anmeldeinformationen durchführen müssen. Wenn Sie den Benutzern neue Software bereitstellen, erstellen Sie eine Anwendungsdefinition für die Anwendung und fügen Sie mit dem Provisioning die Anmeldeinformationen aller Benutzer hinzu, die diese Anwendung verwenden.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Zusammenfassung der Provisioningtasks“ auf Seite 190
- „Erstellen einer Provisioningvorlage“ auf Seite 192
- „Bearbeiten der Provisioningvorlage“ auf Seite 193
- „Provisioning von Anmeldeinformationen“ auf Seite 203
- „Anpassen der Verarbeitung des Provisioning der Anmeldeinformationen“ auf Seite 205
- „Das Credential Provisioning SDK“ auf Seite 205

Zusammenfassung der Provisioningtasks

Wenn Sie die Anmeldeinformationen manipulieren möchten, die im zentralen Speicher für Single Sign-On-aktivierte Anmeldungen gespeichert sind, die in Benutzerkonfigurationen enthalten sind, müssen Sie die folgenden Tasks ausführen:

Task	Siehe Abschnitt
1. Installieren des Moduls **Provisioning** des Password Manager-Dienstes.	„Installieren und Konfigurieren des Password Manager-Dienstes“ im *Citrix Password Manager-Installationshandbuch*.
2. Erstellen einer Benutzerkonfiguration, die den Provisioningdienst verwendet.	„Erstellen von Benutzerkonfigurationen“ auf Seite 107.
3. Erstellen einer Provisioningvorlage.	„Erstellen einer Provisioningvorlage“ auf Seite 192.
4. Importieren der Anmelde-informationen des Benutzers in die Vorlage und Auswählen eines auszuführenden Befehls.	„Bearbeiten der Provisioningvorlage“ auf Seite 193.
5. Verarbeiten der Provisioningdaten.	„Provisioning von Anmeldeinformationen“ auf Seite 203.

Wichtig: Die XML-Datei, mit der Sie das Provisioning der Anmelde-informationen durchführen, enthält sehr vertrauliche Benutzerdaten. Sie sollten die Datei löschen oder auf einen sicheren Standort verschieben, wenn das Provisioning der Anmeldeinformationen abgeschlossen ist.

Wenn Sie die Anmeldeinformationen im zentralen Speicher hinzugefügt, entfernt oder bearbeitet haben, können diese Angaben in der Umgebung verwendet werden. Wenn Benutzer die Agentsoftware starten, werden die Anmeldeinformationen von Single Sign-On-aktivierten Anmeldungen erkannt und den Benutzern zur Verfügung gestellt. Bei der Erstverwendung der Agentsoftware müssen Benutzer nicht die Ersteinrichtung der Anmeldeinformationen durchführen, wenn Sie alle Anmeldeinformationen mit dem Provisioning dem zentralen Speicher hinzugefügt haben.

Wenn Sie die Anmeldeinformationen vieler Benutzer bearbeiten müssen, sollten Sie das Credential Provisioning Software Development Kit (SDK) im Ordner \Support\Provisioning auf der Produkt-CD in Erwägung ziehen. Weitere Informationen finden Sie unter „Das Credential Provisioning SDK“ auf Seite 205.

Hinweis: Das Hinzufügen, Bearbeiten oder Löschen von Anmeldeinformationen im zentralen Speicher kann viele Systemressourcen verbrauchen. Daher sollten Sie das Provisioning der Anmeldeinformationen in Zeiten geringer Auslastung durchführen.

Erstellen einer Provisioningvorlage

Hinweis: Im folgenden Verfahren wird vorausgesetzt, dass Sie eine Benutzerkonfiguration mit mindestens einem der folgenden Objekte erstellt haben: Anwendungsdefinition, Anwendungsgruppe, Kennwortrichtlinie (möglicherweise mit einer optionalen Kennwortgruppe). Außerdem muss das Provisioning ist in der Benutzerkonfiguration aktiviert sein.

Eine Provisioningvorlage ist eine XML-Datei, die Informationen zu den Anwendungen enthält, die in dieser Benutzerkonfiguration enthalten sind:

- Anwendungsgruppe
- Name der Anwendungsdefinition und GUID
- Benutzerinformationen, wie z. B. Benutzername und Kennwort

Sie enthält auch Befehle zum Hinzufügen, Entfernen und Bearbeiten, die Sie beim Importieren der bearbeiteten Vorlage in Password Manager verwenden können.

So erstellen Sie eine Provisioningvorlage

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und wählen Sie **Benutzerkonfigurationen** aus.
3. Wählen Sie eine Benutzerkonfiguration.
4. Klicken Sie im Bereich **Häufige Tasks** auf **Provisioningvorlage erstellen**.
5. Geben Sie im Dialogfeld **Provisioningvorlage erstellen** einen Namen für die Vorlage ein und klicken Sie auf **Speichern**.
6. Klicken Sie auf **OK**, um das Erstellen einer Vorlage im XML-Dateiformat zu bestätigen.

Diese Vorlage enthält Beispiele von Befehlen und Informationen zu der ausgewählten Benutzerkonfiguration. Weitere Informationen finden Sie unter „Bearbeiten der Provisioningvorlage“ auf Seite 193.

Bearbeiten der Provisioningvorlage

Hinweis: Bearbeiten Sie die erstellte Vorlage in einem Texteditor oder einem XML-Dateieditor. In der Provisioningvorlage wird SPML (Service Provisioning Markup Language), ein XML-basierter Standard für den Datenaustausch, verwendet. Wie bei XML müssen Sie sicherstellen, dass alle SPML-Tags oder -Elemente (z. B. „add“) richtig strukturiert ist und die XML-Syntaxregeln einhält. Stellen Sie beispielsweise beim Entfernen von Kommentarzeichen wie !-- und -- sicher, dass die überflüssige spitze Klammern (< oder >) entfernen, da sonst Fehler bei der Verarbeitung der Provisioningvorlage auftreten können. Ausführliche Informationen zu XML finden Sie auf der W3C Website unter http://www.w3.org/. Stellen Sie sicher, dass Sie die entsprechenden Kommentarzeichen (!-- und --) entfernen.

In der Provisioningvorlagendatei im XML-Format können Sie die folgenden Tags und Befehle verwenden.

- „Das Tag „cpm-provision““ auf Seite 194
- „Das Tag <user>“ auf Seite 195
- „Der Befehl <add>“ auf Seite 196
- „Der Befehl <modify>“ auf Seite 198
- „Der Befehl <delete>“ auf Seite 199
- „Der Befehl <remove>“ auf Seite 200
- „Der Befehl <reset>“ auf Seite 201
- „Der Befehl <list-credentials>“ auf Seite 202

Das Tag „cpm-provision“

Hinweis: Sie müssen die gewünschten Tags und Befehle im Provisioningtag <cpm-provision> einschließen (ungefähr auf Zeile 70 in der erstellten XML-Datei):

```
<cpm-provision version="1.0"
xmlns="http://citrix.com/Provision/Import">
Fügen Sie das Tag <user> und Befehle an dieser Stelle ein
</cpm-provision>
```

Beispielsausgabe

Die erstellte Vorlage enthält Folgendes:

- <user> Informationen zum Benutzer, der die Vorlage erstellt hat
- <add> Befehl für den Anwendungsnamen in der Benutzerkonfiguration
- <modify> Befehl mit dem Namen der Anwendungsdefinition

Am Ende der XML-Datei finden Sie Informationen zu der ausgewählten Benutzerkonfiguration, die Sie kopieren und in der Vorlage verwenden können. Beispiel:

```
<user fqdn="DOMÄNE\Fred-Admin">

<!--Application Group: PNA-->

<!--Application Definition: Citrix GoToMeeting-->

<!--<add>

    <application name="Citrix GoToMeeting">0998ac2c-baa5-4103-809a-
b2daeea047f3</application>

    <name>Citrix GoToMeeting</name>

    <description>Citrix GoToMeeting Login</description>

    <hidden-description>Citrix GoToMeeting ausgeblendete
Beschreibung</hidden-description>

    <userID>Benutzer-ID</userID>

    <password>Kennwort</password>

</add>-->

<!--<modify>

    <credential-id>00000000-0000-0000-0000-000000000000</
credential-id>

    <name>Citrix GoToMeeting</name>

    <description>Citrix GoToMeeting Login</description>
```

```
    <hidden-description>Citrix GoToMeeting ausgeblendete
Beschreibung</hidden-description>

    <userID>Benutzer-ID</userID>

    <password>Kennwort</password>

</modify>-->

</user>
```

Sie können beispielsweise die Benutzerinformationen zwischen den Tags <user> und </user> kopieren, das Kommentarzeichen entfernen und sie für jeden Benutzer bearbeiten, für den Sie Anmeldeinformationen hinzufügen möchten.

Hinweis: Im obigen Beispiel ist `<user fqdn="DOMÄNE\Fred-Admin">` die Domäne und der Benutzername des Benutzers, der die Vorlage erstellt hat. Sie können diese Informationen als Kommmentar markieren oder löschen, wenn Sie diese Angaben nicht in der Vorlage speichern möchten.

Das Tag <user>

Mit dem Tag <user> fügen Sie die Domäne und den Benutzernamen für jeden Benutzer hinzu, für dessen Anmeldeinformationen für die Anwendung Sie das Provisioning verwenden möchten. Sie müssen für jeden Benutzer, für den Sie das Provisioning verwenden, ein Tag <user> angeben. Jedes <user>-Tag enthält auch die Befehle, die für das Konto ausgeführt werden.

Die Befehle haben die folgende Syntax:

```
<user fqdn="DieDomäne\BenutzerID">

    <Befehl>

</user>
```

Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an, der hinzugefügt wird.
Benutzer-ID	Gibt den Benutzernamen des Benutzers an, der hinzugefügt wird.
Befehl	Gibt die Befehle an, die für diesen Benutzer ausgeführt werden können: • <add> • <modify> • <delete> • <remove> • <reset> • <list-credentials>

Der Befehl <add>

Mit dem Befehl <add> fügen Sie einen Benutzernamen und ein Kennwort hinzu, die für Anwendungen benötigt werden, die in der Benutzerkonfiguration enthalten sind.

Die Befehle haben die folgende Syntax:

```
<add>

    <application name="%ANWENDUNGSNAME%>%ANWENDUNGS-
GUID%</application>

    <name>%ANMELDEINFORMATIONEN%</name>

    <description>LangeBeschreibung</description>

    <hidden-description>%ANWENDUNGSNAME% ausgeblendete Beschreibung
</hidden-description>

    <userID>Benutzer-ID</userID>

    <password>Kennwort</password>

    <custom-field index="1" label="%BESCHRIFTUNG%">
Benutzerdefiniertes_Feld_1 </custom-field>

    <custom-field index="2" label="%BESCHRIFTUNG%">
Benutzerdefiniertes_Feld_2 </custom-field>

</add>
```

Wobei Folgendes gilt:

<application>	Erforderlich. Das Element <application> und die Attribute werden normalerweise automatisch beim Erstellen einer Vorlage erstellt. Das Attribut name= ist optional. • *%ANWENDUNGSNAME%* ist der Name der Anwendungsdefinition in der ausgewählten Benutzerkonfiguration. • *%ANWENDUNGS-GUID%* ist die GUID der Anwendung, die übereinstimmen muss.
<name>	Erforderlich. Das Element <name> und die Attribute werden normalerweise automatisch erstellt. • *%ANMELDEINFORMATIONEN%* ist der Name der Anwendung in der Anwendungsdefinition.
<description>	Optional. Geben Sie eine Beschreibung für die Benutzerkonfiguration ein.
<hidden-description>	Optional. Geben Sie Text ein.
<userID>	Erforderlich. *Benutzer-ID* ist der Benutzername des Benutzers, den Sie hinzufügen.
<password>	Erforderlich. *Kennwort* ist das Kennwort des Benutzers, den Sie hinzufügen.
<custom-field>	Erforderlich, wenn ein weiteres Feld für die Authentifizierung benötigt wird (z. B. für ein Feld, in dem der Benutzer die Domäne eingeben muss). Sie können beliebig viele benutzerdefinierte Felder für die Anwendung angeben.

Der Befehl <modify>

Mit dem Befehl <modify> bearbeiten Sie einen Benutzernamen und ein Kennwort, die für Anwendungen benötigt werden, die in der Benutzerkonfiguration enthalten sind.

Wichtig: Für diesen Befehl müssen die Anmeldeinformationen des Benutzers eingegeben werden. Sie können die Anmeldeinformationen mit dem Befehl <list-credentials> abrufen, bevor Sie den Befehl <modify> verwenden. Weitere Informationen finden Sie unter „Der Befehl <list-credentials>“ auf Seite 202.

Schließen Sie nur die Elemente ein, die Sie bearbeiten möchten:

- Löschen Sie die Zeile, wenn ein Wert nicht geändert wird. Beispiel: Löschen Sie das Element <name>, um den Namen der Anwendung unverändert zu lassen.
- Wenn Sie einen Wert ändern möchten, geben Sie den Wert in der Vorlage an. Beispiel: Schließen Sie das Element <name> ein, um einen neuen Anwendungsnamen anzugeben.
- Ein Wert wird entfernt, wenn Sie das Elemetn ohne einen Wert einschließen. Beispiel. Verwenden Sie <description></description>, um die aktuelle Beschreibung zu löschen.

Die Befehle haben die folgende Syntax:

```
<modify>

    <credential-id>%ANMELDEINFORMATIONEN-ID%</credential-id>

    <name>%ANMELDEINFORMATIONEN%</name>

    <description>LangeBeschreibung</description>

    <hidden-description>%ANWENDUNGSNAME% ausgeblendete Beschreibung
</hidden-description>

    <userID>Benutzer-ID</userID>

    <password>Kennwort</password>

    <custom-field index="1" label="%BESCHRIFTUNG%">
Benutzerdefiniertes_Feld_1 </custom-field>

    <custom-field index="2" label="%BESCHRIFTUNG%">
Benutzerdefiniertes_Feld_2 </custom-field>

</modify>
```

Wobei Folgendes gilt:

<credential-id>	Erforderlich. Der Wert für Anmeldeinformationen-GUID *%ANMELDEINFORMATIONEN-ID%* des Benutzers muss mit dem Wert übereinstimmen, der vom Befehl <list-credentials> zurückgegeben wird. Weitere Informationen finden Sie unter „Der Befehl <list-credentials>“ auf Seite 202.
<name>	Optional. Das Element <name> und die Attribute werden normalerweise automatisch erstellt. • *%ANMELDEINFORMATIONEN%* ist der Name der Anwendung in der Anwendungsdefinition.
<description>	Optional. Geben Sie eine Beschreibung für die Benutzerkonfiguration ein.
<hidden-description>	Optional. Geben Sie Text ein.
<userID>	Erforderlich. *Benutzer-ID* ist der Benutzername des Benutzers, den Sie bearbeiten.
<password>	Erforderlich. *Kennwort* ist das Kennwort des Benutzers, den Sie bearbeiten.
<custom-field>	Erforderlich, wenn ein weiteres Feld für die Authentifizierung benötigt wird (z. B. für ein Feld, in dem der Benutzer die Domäne eingeben muss). Sie können beliebig viele benutzerdefinierte Felder für die Anwendung angeben.

Der Befehl <delete>

Mit dem Befehl <delete> löschen Sie die Anmeldeinformationen eines Benutzers für eine Single Sign-On-aktivierte Anwendung.

Wichtig: Für diesen Befehl müssen die Anmeldeinformationen des Benutzers eingegeben werden. Sie können die Anmeldeinformationen mit dem Befehl <list-credentials> abrufen, bevor Sie den Befehl <delete> verwenden. Weitere Informationen finden Sie unter „Der Befehl <list-credentials>“ auf Seite 202.

Die Befehle haben die folgende Syntax:

```
<user fqdn="DieDomäne\BenutzerID">
    <delete>
        <credential-id>%ANMELDEINFORMATIONEN-ID%</credential-id>
    </delete>
</user>
```

Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.
<credential-id>	Erforderlich. Der Wert für Anmeldeinformationen-GUID *%ANMELDEINFORMATIONEN-ID%* des Benutzers muss mit dem Wert übereinstimmen, der vom Befehl <list-credentials> zurückgegeben wird. Weitere Informationen finden Sie unter „Der Befehl <list-credentials>“ auf Seite 202.

Der Befehl <remove>

Hinweis: Dieser Befehl ähnelt dem Task **Benutzerdaten aus dem zentralen Speicher löschen** in der Password Manager Console. Weitere Informationen finden Sie unter „Benutzerdaten aus dem zentralen Speicher löschen“ auf Seite 143.

Mit dem Befehl <remove> entfernen Sie Benutzerdaten und -informationen aus dem zentralen Speicher. Verwenden Sie den Befehl, wenn ein Benutzer nicht mehr im Unternehmen arbeitet. Der lokaler Speicher der Anmeldeinformationen auf dem PC des Benutzers bleibt intakt, bis er explizit von einem Administrator oder Benutzer gelöscht wird.

Die Befehle haben die folgende Syntax:

```
<user fqdn="DieDomäne\BenutzerID">
    <remove />
</user>
```

Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.

Der Befehl <reset>

Hinweis: Dieser Befehl ähnelt dem Task **Benutzerdaten zurücksetzen** in der Password Manager Console. Weitere Informationen finden Sie unter „Benutzerdaten zurücksetzen“ auf Seite 141.

Die Agentsoftware verarbeitet jeden Befehl zum Zurücksetzen, wenn der Agent startet oder neu gestartet wird (wenn das Programm aktuell auf dem PC des Benutzers ausgeführt wird). Sonst verarbeitet die Agentsoftware alle anderen Provisioningbefehle, wenn der Agent gestartet oder neu gestartet wird, wenn der Benutzer im Anmeldungsmanager der Agentsoftware auf **Aktualisieren** klickt, oder wenn der Benutzer im Kontextmenü des Agentsymbols auf **Aktualisieren** klickt.

Wenn die Warteschlange einen Befehl **Zurücksetzen** enthält, und der Benutzer auf **Aktualisieren** klickt, wird dem Benutzer in einer Meldung angezeigt, dass die Benutzerdaten zurückgesetzt wurden und ein Neustart von Password Manager Agent erforderlich ist.

Mit dem Befehl <reset> setzen Sie Anmeldeinformationen des Benutzers im zentralen Speicher zurück, wodurch dieser Benutzer auf den Originalzustand zurückgesetzt wird. Bei zentralen Speichern, die nicht in Active Directory erstellt sind, bleiben die Benutzerordner gespeichert, aber alle Benutzerdaten (Anmeldeinformationen, Sicherheitsfragen und Antworten usw.) werden gelöscht. In zentralen Speichern, die unter Active Directory erstellt sind, werden die Benutzerdaten gelöscht, und der Benutzer wird markiert, dass die Daten zurückgesetzt wurden.

Die Befehle haben die folgende Syntax:

```
<user fqdn="DieDomäne\BenutzerID">
    <reset />
</user>
```

Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an.

Der Befehl <list-credentials>

Mit dem Befehl <list-credentials> rufen Sie die Anmeldeinformationen des Benutzers für jede Anwendung ab, die in der zugeordneten Anwendungsdefinition enthalten ist. Bei den Befehlen <modify> und <delete> müssen Sie die abgerufene Anmeldeinformationen-GUID als Wert für den Parameter *%ANMELDEINFORMATIONEN-ID%* verwenden. (Weitere Informationen finden Sie unter „Der Befehl <modify>“ auf Seite 198 und „Der Befehl <delete>“ auf Seite 199.)

Die Identnummer, die von diesem Befehl abgerufen wird, ist eine Anmeldeinformationen-GUID.
Beispiel: 634EE015-10C2-4ed2-80F5-75CCA9AA5C11.

Die Befehle haben die folgende Syntax:

```
<user fqdn="DieDomäne\BenutzerID">
    <list-credentials />
</user>
```

Wobei Folgendes gilt:

DieDomäne	Gibt den Namen der Domäne des Benutzers an, der hinzugefügt wird.
Benutzer-ID	Gibt den Namen der Domäne des Benutzers an, der hinzugefügt wird.

Provisioning von Anmeldeinformationen

Führen Sie in der Konsole die Provisioningtasks durch, die in der XML-Datei aufgeführt sind. Password Manager prüft die Syntax jedes Befehls, führt die Befehle aus und fügt die Daten dem zentralen Speicher hinzu oder bearbeitet die Daten im zentralen Speicher.

So verarbeiten Sie die Provisioningvorlage

Achtung: Schließen Sie das Dialogfeld für das Verarbeiten des Provisioning erst, wenn das Provisioning ganz angehalten oder abgeschlossen ist. Das Schließen des Dialogfelds hält die Verarbeitung des Provisioning nicht an. Wenn Sie das Dialogfeld während der Verarbeitung des Provisioning schließen, können Sie keine Informationen erfassen oder den Prozess vor dem Abschluss anhalten.

---

1. Klicken Sie auf **Start** > **Alle Programme** > **Citrix** > **Managementkonsolen** > **Access Management Console**.
2. Erweitern Sie den Knoten **Password Manager** und dann den Knoten **Benutzerkonfigurationen**.
3. Wählen Sie eine Benutzerkonfiguration oder eine Anwendungsgruppe einer Benutzerkonfiguration aus.
4. Klicken Sie unter **Häufige Tasks** auf **Provisioning ausführen**.

   Der **Assistent für das Provisioning** wird angezeigt.
5. Klicken Sie auf **Weiter**.

6. Geben Sie den Namen der Provisioning-XML-Datei ein oder klicken Sie auf **Durchsuchen**. Klicken Sie dann auf **Weiter**.

   Password Manager prüft die XML-Datei.

   - Wenn keine Syntaxfehler bestehen, wird eine Zusammenfassung der Änderungen angezeigt, die Sie machen können. Sie können die Zusammenfassung speichern.
   - Wenn Syntax- oder andere Fehler bestehen, wird ein Fehlerprotokoll erstellt. Sie können das Fehlerprotokoll speichern und dann auf **Abbrechen** klicken, um den Assistenten zu schließen.

7. Wenn keine Fehler bestehen, klicken Sie auf **Weiter**, um die Befehle in der Datei auszuführen.

   Wenn die Informationen im zentralen Speicher geändert werden, werden Fehler angezeigt, die aufgrund des Provisioning aufgetreten sind. Klicken Sie auf **Abbrechen**, wenn Sie das Provisioning beenden möchten. Wenn Password Manager das Ende des aktuellen Abschnitts der verarbeiteten Daten erreicht (in der Standardeinstellung werden Daten in Gruppen von 50 Codezeilen verarbeitet), wird das Provisioning beendet.

8. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden. Sie können auch auf **In Datei speichern** klicken, um die Provisioningergebnisse zu speichern.

Anpassen der Verarbeitung des Provisioning der Anmeldeinformationen

---

Achtung: In diesen Informationen werden manuell bearbeitete Registrierungs-einstellungen beschrieben. Sichern Sie die Registrierung immer ab, bevor Sie Änderungen vornehmen.

Wenn Sie Password Manager für das Provisioning von Anmeldeinformationen verwenden, werden die Informationen in der Standardeinstellung in Serien von 50 Befehlen mit einem Timeout von 100.000 Millisekunden verarbeitet. Sie können die folgenden Registrierungsschlüssel bearbeiten, um diese Standardwerte zu ändern:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
\MetaFrame Password Manager\Console\Provisioning\BatchSize

Typ: DWORD

Standardwert bei keiner Eingabe: 50

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix
\MetaFrame Password Manager\Console\Provisioning\ServiceTimeout

Typ: DWORD

Standardwert in Millisekunden bei keiner Eingabe: 100000

Das Credential Provisioning SDK

Das Credential Provisioning-SDK im Ordner \Support\Provisioning auf der Produkt-CD enthält eine Beschreibung aller APIs, die verfügbar sind, wenn Sie das Modul Provisioning des Password Manager-Dienstes installieren. Mit diesem SDK und dem darin enthaltenen Beispielcode können Sie eigene Provisioningclients erstellen und mit Password Manager verwenden.

Hotdesktop: Desktopfreigabeumgebung für Benutzer

Hinweis: Hotdesktop wird nur unter Microsoft Windows 2000 Professional, Microsoft Windows XP Embedded und Microsoft Windows XP Professional, Service Pack 2 (32 Bit) unterstützt. Die Funktion wird nicht unter 64-Bit-Betriebssystemen oder Serverbetriebssystemen unterstützt.

Mit der Hotdesktop-Funktion von Citrix Password Manager können Benutzer effizient und sicher Arbeitsstationen gemeinsam verwenden. Hotdesktop erweitert die Windows-Standardbenutzerumgebung um folgende Funktionen:

- Schnelle Windows-Authentifizierung mit dem interaktiven GINA-Standarddialogfeld für die Anmeldung
- Ausführen von Single Sign-On-aktivierten Anwendungen in der interaktiven Benutzer-Shell mit Anmeldeinformationen des Benutzers für Citrix Password Manager
- Abmelden von der Hotdesktop-Arbeitsstation, damit andere Benutzer Anwendungen ausführen können

Hotdesktop verbindet die Flexibilität eines schnellen Benutzerwechsels mit der Sicherheit der Single Sign-On-Funktion von Password Manager. Die Hotdesktop-Funktion wird nicht standardmäßig installiert. Sie können die Funktion bei der Agentinstallation auswählen. Bestehende Agentbereitstellungen können auch für die Verwendung von Hotdesktop aktualisiert werden. Vor der Implementierung von Hotdesktop müssen Sie die Anwendung entsprechend den vorliegenden Umgebungs- und Unternehmensanforderungen konfigurieren.

In diesem Abschnitt werden die folgenden Themen behandelt:

- „Zusammenfassung der Hotdesktop-Tasks" auf Seite 209
- „Prozessablauf beim Starten und Beenden von Hotdesktop" auf Seite 211
- „Erstellen eines Hotdesktop-Kontos" auf Seite 214
- „Anforderungen für Anwendungen, die mit Hotdesktop verwendet werden" auf Seite 217
- „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer" auf Seite 219
- „Einstellungen der Benutzerkonfiguration für Hotdesktop" auf Seite 229
- „Installieren von Hotdesktop" auf Seite 232
- „Deinstallieren von Hotdesktop" auf Seite 234
- „Zusammenwirken mit Citrix Presentation Server Clients" auf Seite 238
- „Anzeigen von Hotdesktop-Benutzerprofilen" auf Seite 239
- „Herunterfahren von Hotdesktop-Arbeitsstationen" auf Seite 239
- „Arbeiten ohne AutoAdminLogon-Unterstützung" auf Seite 240
- „Ändern des Kennworts für das Hotdesktop-Konto" auf Seite 241
- „Informationen zu Hotdesktop im Web" auf Seite 241

Zusammenfassung der Hotdesktop-Tasks

Vor der Implementierung von Hotdesktop müssen Sie Folgendes ausführen:

- Erstellen eines Hotdesktop-Kontos
- Erstellen von Benutzerkonfigurationen mit speziellen Hotdesktop-bezogenen Einstellungen zum Anpassen der Hotdesktop-Benutzererfahrung
- Definieren des Hotdesktop-Verhaltens beim Starten und Beenden, einschließlich:
    - Festlegen der Anwendungen, die beim Starten geöffnet werden bzw. von denen Hotdesktop-Anmeldeinformationen und -Berechtigungen (Benutzer- bzw. Hotdesktop-Konto) verwendet werden
    - Festlegen der Anwendungen, die für schnelle Benutzerwechsel dauerhaft (d. h. auch nach dem Abmelden von Benutzern) ausgeführt werden bzw. nach dem Abmelden von Benutzern beendet werden, einschließlich persönlicher optionaler Bereinigungsskripte oder Anwendungen zum Löschen von Benutzerinformationen zwischen Sitzungen

Führen Sie die folgenden Aufgaben aus, um Hotdesktop zu konfigurieren und zu aktivieren:

Aufgabe	Siehe Abschnitt
1. Erstellen Sie ein Hotdesktop-Konto, das für jede Arbeitsstation bzw. jedes Clientgerät, auf dem Hotdesktop ausgeführt wird, verfügbar ist.	„Erstellen eines Hotdesktop-Kontos“ auf Seite 214
2. Legen Sie fest, welche Single Sign-On-aktivierten Anwendungen in der Hotdesktop-Umgebung ausgeführt werden.	„Anforderungen für Anwendungen, die mit Hotdesktop verwendet werden“ auf Seite 217
3. Legen Sie fest, wie Anwendungen unter Hotdesktop ausgeführt werden und konfigurieren Sie die Hotdesktop-Benutzerumgebung.	• „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer“ auf Seite 219 • „Die Datei session.xml“ auf Seite 221 • „Die Datei process.xml“ auf Seite 225
4. Erstellen oder ändern Sie eine Benutzerkonfiguration für die Auswahl von Hotdesktop-Optionen.	• „Einstellungen der Benutzerkonfiguration für Hotdesktop“ auf Seite 229 • „Agentverhalten konfigurieren“ auf Seite 120 • „Erweiterte Einstellungen“ auf Seite 122
5. Installieren Sie die Agentsoftware mit der ausgewählten Hotdesktop-Funktion.	„Installieren von Hotdesktop“ auf Seite 232
6. Deinstallieren Sie Hotdesktop bei Bedarf.	„Deinstallieren von Hotdesktop“ auf Seite 234

Prozessablauf beim Starten und Beenden von Hotdesktop

In diesem Abschnitt werden die folgenden Themen beschrieben:

- „Ereignisse zum Starten und Beenden von Hotdesktop“ auf Seite 211
- „Problembehandlung beim benutzerseitigen Start von Hotdesktop“ auf Seite 212

Ereignisse zum Starten und Beenden von Hotdesktop

Im Folgenden werden die Ereignisse beschrieben, die im Zusammenhang mit dem Starten und Beenden von Hotdesktop auftreten. Wenn die Arbeitsstation bzw. das Clientgerät gestartet wird, wird es automatisch am Hotdesktop-Konto angemeldet, sodass das Gerät im Desktopfreigabemodus ausgeführt werden kann.

Hinweis: Das Hotdesktop-Konto bleibt durchgehend aktiviert. Benutzer sind nicht berechtigt, das Hotdesktop-Konto zu beenden.

---

1. Ein Hotdesktop-Benutzer meldet sich an der Arbeitsstation an und gibt einen Benutzernamen und ein Kennwort ein bzw. verwendet eine starke Authentifizierungsmethode, wie z. B. eine Smartcard.
2. Wenn der Benutzer authentifiziert wurde, beginnt die Hotdesktop-Sitzung.
3. Password Manager wird gestartet. Die Agentsoftware synchronisiert die Daten mit dem zentralen Speicher. Dies stellt sicher, dass der Benutzer die aktuellen Anwendungsdefinitionen, Kennwortrichtlinien und anderen agentbezogenen Einstellungen besitzt.
4. Die Datei session.xml wird gelesen und alle Anwendungen, für die Sie festgelegt haben, dass sie unter dem Hotdesktop-Konto oder dem Hotdesktop-Benutzerkonto ausgeführt werden, werden gestartet. Weitere Informationen finden Sie unter „Die Datei session.xml“ auf Seite 221. Bei den Anwendungen kann es sich sowohl um lokale Anwendungen als auch um Remoteanwendungen handeln, die mit Presentation Server veröffentlicht wurden. Der Benutzer greift auf die Anwendungen zu, um die ihm übertragenen Aufgaben auszuführen.

5. Der Hotdesktop-Benutzer meldet sich ab.

Hinweis: Wenn Benutzer eine Arbeitsstation im Leerlauf lassen, initiiert Hotdesktop ein Sitzungstimeout. In der Password Manager Console legen Sie fest, wie lange eine Arbeitsstation inaktiv bleiben kann. Wenn das Intervall überschritten wird, sperrt Hotdesktop die Arbeitsstation. Wenn noch weitere Zeit vergangen ist, und der Benutzer nicht zurückkehrt, beendet Hotdesktop die Sitzung. Weitere Informationen finden Sie unter „Festlegen von Timeoutoptionen für Hotdesktop-Sitzungen“ auf Seite 230.

---

6. Die Anwendungen werden weiterhin ausgeführt oder beendet. Dies hängt von den Einstellungen in der Datei process.xml ab. Weitere Informationen finden Sie unter „Die Datei process.xml“ auf Seite 225.
7. Password Manager wird beendet.
8. In der Datei session.xml angegebene Skripte zum Beenden werden ausgeführt.
9. Die Hotdesktop-Sitzung wird beendet.

Problembehandlung beim benutzerseitigen Start von Hotdesktop

Wenn ein Benutzer sich an einem Computer mit Password Manager Agent anmeldet, der mit Hotdesktop konfiguriert ist, werden die in der Datei session.xml angegebenen Startskripte möglicherweise ausgeführt, bevor der Start von Password Manager Agent abgeschlossen ist.

Hotdesktop wartet beim Start 30 Sekunden auf den Start der Agentsoftware, bevor die Startskripte ausgeführt werden. Nach 30 Sekunden werden die Startskripte ausgeführt, selbst wenn Password Manager Agent noch nicht vollständig funktionsbereit ist.

Diese Situation tritt am wahrscheinlichsten bei der Erstanmeldung des Benutzers auf (d. h. bei der Erstverwendung der Software durch den Benutzer), wenn der Password Manager-Administrator eine Liste von Anwendungen festgelegt hat, für die eine Registrierung von Anmeldeinformationen oder ein Beantworten von Sicherheitsfragen erforderlich ist. In diesem Fall gilt folgender Handlungsablauf:

1. Der Benutzer meldet sich am Computer oder Clientgerät mit der Agentsoftware an und wird in einer Meldung aufgefordert, die Anmeldeinformationen für die aufgelisteten Anwendungen oder Antworten auf Sicherheitsfragen einzugeben.
2. Während er diese Aufgaben ausführt, vergehen 30 Sekunden und die Hotdesktop-Startskripte werden ausgeführt. Je nach den Anwendungen, die in den Startskripten von session.xml angegeben sind, können verschiedene Fenster geöffnet und geschlossen werden.
3. Wenn die Startskript-Fenster vom Computer wiederholt aufgerufen werden, kann dies bei Benutzern zu Frustrationen führen.
4. Wenn die Startskripte abgeschlossen sind, wird eine Fehlermeldung angezeigt. Sie lautet in etwa: „Ein oder mehrere Fehler sind aufgetreten. Weitere Informationen finden Sie im Ereignisprotokoll."

Auch wenn Benutzer dieses Verhalten unter Umständen als frustrierend empfinden, werden dadurch weder die Benutzerdaten noch die Arbeitsumgebung oder Password Manager beschädigt.

Empfehlen Sie den Benutzern daher, die Anmeldeinformationen und Antworten auf Sicherheitsfragen erst nach der Anzeige dieser Fehlermeldung zu registrieren. Sie können die Fehlermeldung dann schließen und die Anmeldung und Registrierung abschließen.

Wenn nach der Fehlermeldung und Registrierung eine Anwendung aus der Datei session.xml nicht geöffnet wurde, sollten sich Benutzer abmelden und erneut am Konto anmelden. Dieses Schema startet die Startskripte für Hotdesktop erneut, die ohne Störung ausgeführt werden, da die Registrierung abgeschlossen ist und den Prozess nicht weiter verzögert.

Weitere Informationen zu Startskripten und Skripten zum Beenden finden Sie unter „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer" auf Seite 219.

Erstellen eines Hotdesktop-Kontos

Sie müssen für Clientgeräte oder Arbeitsstationen, auf denen Hotdesktop ausgeführt werden soll, ein Hotdesktop-Konto erstellen. Dieses Hotdesktop-Konto kann ein Domänenkonto oder ein lokales Konto auf dem Gerät sein. Bei der Installation von Hotdesktop auf dem Clientgerät geben Sie Anmeldeinformationen für das Hotdesktop-Konto ein. Beim Start wird das Clientgerät bzw. die Arbeitsstation automatisch am Hotdesktop-Konto angemeldet und kann im Hotdesktop-Freigabemodus für Arbeitsstationen ausgeführt werden.

Benutzersitzungen werden „über" der Windows-Sitzung des Hotdesktop-Kontos ausgeführt (Benutzer können das Hotdesktop-Konto nur ändern, wenn Sie es Ihnen ausdrücklich gestatteten. Benutzer starten eine Hotdesktop-Sitzung durch Eingabe der Windows-Domänenanmeldeinformationen. In einer Hotdesktop-Umgebung wird das Windows-Konto eines Benutzers als *Hotdesktop-Benutzer* bezeichnet.

Richtlinien für das Hotdesktop-Konto

Beachten Sie beim Erstellen eines Hotdesktop-Kontos die folgenden Richtlinien:

- Stellen Sie sicher, dass das Konto nicht zur Gruppe der lokalen oder Domänenadministratoren gehört.
- Das Hotdesktop-Konto kann ein lokales oder ein Domänenkonto sein. Alle Berechtigungen, die für das Hotdesktop-Konto gelten, sind für den Hotdesktop-Benutzer nur für die von Ihnen angegebenen Anwendungen verfügbar. Sie können also angeben, welche Anwendungen mit Anmeldeinformationen für das Hotdesktop-Konto und welche mit den Windows-Domänenanmeldeinformationen des Benutzers gestartet werden.
- Bei der Installation von Hotdesktop werden der Anmeldename und die Domäne des Hotdesktop-Kontos geprüft. Stellen Sie beim Erstellen des Kontos sicher, dass Sie die Option **Kennwort läuft nie ab** auswählen. Verwenden Sie keine abgelaufenen Anmeldeinformationen.
- Stellen Sie sicher, dass dem Konto nur eingeschränkte Privilegien gewährt werden, Schränken Sie die Berechtigungen nur auf die Hotdeskop-Verwendung ein.

- Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen. Wenn Sie ein lokales Konto verwenden, geben Sie den Hostnamen des Gerätes an.

- Sie sollten das Hotdesktop-Konto „Hotdesktop" nennen. Dies stellt sicher, dass den Benutzern beim Abmelden von der Windows 2000-Umgebung klar angezeigt wird, dass sie sich von Hotdesktop abmelden. Wenn Sie statt „Hotdesktop" einen weniger aussagekräftigen Namen verwenden, kann die angezeigte Meldung für die Benutzer beim Abmelden verwirrend sein. Bei mehreren Gruppen von Hotdesktop-Benutzern können Sie für jedes Hotdesktop-Konto einen entsprechenden Namen wählen, z. B. „Hotdesktop Marketing", „Hotdesktop Buchhaltung" usw.

Organisieren von Hotdesktop-Benutzern

Wenn Sie beabsichtigen, Hotdesktop bereitzustellen, sollten Sie zunächst die Benutzerumgebung einrichten. Sie können Hotdesktop-Benutzer zum Beispiel in Active Directory in mehreren Organisationseinheiten oder Gruppen zusammenfassen. Außerdem können Sie Benutzer, die Hotdesktop-Benutzer sind und auch eigene Arbeitsstation verwenden, in mehrere Gruppen unterteilen (und diesen Gruppen Prioritäten zuweisen).

Sie können dann Hotdesktop-Einstellungen, Anwendungsdefinitionen, Kennwortrichtlinien und anderen Konfigurationsangaben auf mehrere Hotdesktop-Benutzer in diesen Organisationseinheiten anwenden.

Einschränken von Benutzerrechten

Da das Hotdesktop-Gerät von allen Hotdesktop-Benutzern gemeinsam verwendet wird, müssen Sie ggf. Berechtigungen beschränken, damit Benutzer die ihnen zugeordneten Anwendungen verwenden können. So sollten Hotdesktop-Benutzer nicht berechtigt sein, das Gerät herunterzufahren. Nur Mitglieder der Administratorgruppe sollten über diese Berechtigung verfügen.

Hotdesktop, Smartcards und Schlüsselwiederherstellung

Hinweis: Wählen Sie die Datenschutzoption **Smartcardzertifikat** der Benutzerkonfiguration, wenn Benutzer Smartcards in der Hotdesktop-Umgebung verwenden.

Wenn Sie Hotdesktop in einer Umgebung bereitstellen, in der sich Benutzer über Smartcards anmelden, wählen Sie für diese Benutzer nicht die Option **Benutzer zur Eingabe des alten Kennworts auffordern** als einzige Schlüsselwiederherstellungs- und Datenschutzmethode. Benutzer in diesen Umgebungen können das alte Kennwort nicht korrekt eingeben und hätten daher keinen Zugriff auf das System. Sie vermeiden dieses Problem, indem Sie zur Schlüsselwiederherstellung die Option **Automatische Schlüsselwiederherstellung** wählen oder eine fragenbasierte Authentifizierung als Option anbieten.

Weitere Informationen finden Sie unter:

- „Richtlinien für mehrere primäre Authentifizierungsmethoden und Methoden zum Schutz der Anmeldeinformationen der Benutzer“ im *Password Manager-Installationshandbuch*
- „Erstellen von Benutzerkonfigurationen“ auf Seite 107
- „Benutzerauthentifizierung und Identitätsprüfung“ auf Seite 151
- „Verwalten der fragenbasierten Authentifizierung“ auf Seite 159

Anforderungen für Anwendungen, die mit Hotdesktop verwendet werden

Anwendungen, die in einer Hotdesktop-Umgebung verwendet werden, müssen die folgenden Voraussetzungen erfüllen:

- Anwendungen, für die Anmeldeinformationen des Benutzers benötigt werden, müssen in Anwendungsdefinitionen und Benutzerkonfigurationen für Password Manager eingerichtet sein.
- Anwendungen, die vom Hotdesktop-Konto gestartet werden, müssen in der interaktiven Windows-Umgebung ausführbar sein. Bei diesem Szenario benötigen die Anwendungen (und die Hotdesktop-Benutzer) Zugriff auf die Benutzerprofile, Netzwerkfreigaben und auf andere Ressourcen, die dem Hotdesktop-Konto zugeordnet sind.
- Die Anwendungen müssen in der Lage sein, sich ordnungsgemäß zu beenden, wenn sie dazu aufgefordert werden. Hotdesktop beendet Anwendungen mit ähnlichen Verfahren wie bei der Abmeldung von einer interaktiven Windows-Sitzung. Das ordnungsgemäße Beenden von Anwendungen ist in einer Hotdesktop-Umgebung besonders wichtig, da die Anwendung unter Umständen viele Male verwendet wird, bevor die Arbeitsstation oder das Clientgerät heruntergefahren wird.

- Alle Anwendungen, die im Profil des Benutzers vertrauliche Daten speichern oder zum Ändern von Einstellungen auf das Profil des Benutzers zugreifen müssen, sollten als Hotdesktop-Benutzerkonto ausgeführt werden. Anwendungen, die „gemeinschaftliche" Konfigurations-informationen gemeinsam nutzen können, können als Hotdesktop-Konto ausgeführt werden. Mit dem in der Datei session.xml definierten Skript zum Beenden können Administratoren sicherstellen, dass benutzer-spezifische Dateien am Ende jeder Sitzung entfernt werden. Weitere Informationen finden Sie unter „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer" auf Seite 219.

Wichtig: Wenn Password Manager Anmeldeinformationen in einer Hotdesktop-Umgebung für Terminalemulatoren senden soll, die Informationen in der Registrierungsstruktur HKEY_CURRENT_USER speichern, müssen Sie diese Anwendungen als Hotdesktop-Benutzerkonto ausführen. Sie können im Abschnitt **ShellExecute** der Datei process.xml festlegen, welche Terminalemulatoren als Hotdesktop-Benutzerkonto ausgeführt werden. Wenn ein Terminalemulator bei Sitzungsbeginn ausgeführt wird, legen Sie dies im entsprechenden Startskriptabschnitt in der Datei session.xml fest. Terminalemulatoren müssen im Startskript als Hotdesktop-Benutzerkonto ausgeführt werden. Weitere Informationen finden Sie unter „Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer" auf Seite 219.

Festlegen des Anwendungsverhaltens für Hotdesktop-Benutzer

Von Password Manager werden die zwei Dateien zur Verfügung gestellt, mit denen das Anwendungsverhalten in Hotdesktop-Umgebungen gesteuert werden: session.xml und process.xml.

In diesem Abschnitt werden die folgenden Themen beschrieben:

Hinweis: Siehe auch „Prozessablauf beim Starten und Beenden von Hotdesktop“ auf Seite 211.

Einführung

Wichtig: Sie können für einen Prozess nicht festlegen, dass er in der Datei session.xml als Hotdesktop-Konto ausgeführt wird und ihn anschließend in der Datei process.xml als Hotdesktop-Benutzer definieren. Einträge in der Datei session.xml haben Vorrang vor den Einträgen, die Sie in der Datei process.xml unter <shellexecute_processes> vornehmen.

- Um sich am PC, an der Arbeitsstation oder am Clientgerät für Verwaltungszwecke anzumelden (z. B. zum Bearbeiten der Datei process.xml), halten Sie während des Windows-Startvorganges die Umschalttaste gedrückt. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.

- Wenn Sie innerhalb einer Hotdesktop-Benutzersitzung die Hotdesktop-Datei session.xml, Kennwortablaufskripte oder andere Skripte sowie ausführbare Dateien oder Batchdateien ausführen, werden folgende Umgebungsvariablen nicht unterstützt: APPDATA, HOMEDRIVE, HOMEPATH, HOMESHARE und LOGONSERVER. Wenn eine dieser nicht unterstützten Variablen verwendet wird, kann das Skript, die Anwendung oder die ausführbare Datei unter Umständen nicht ausgeführt werden. Um dieses Problem zu vermeiden, sollten Anwendungen in einer Hotdesktop-Benutzersitzung nicht auf Umgebungsvariablen zugreifen, die nicht unterstützt werden.
- Sie müssen die Benutzer anweisen, die Anwendungen zu beenden, die als permanente Prozesse festgelegt sind. Wenn z. B. ein Benutzer einen permanenten Prozess startet, eine Datei erstellt und die Datei beim Beenden der Hotdesktop-Sitzung offen lässt, kann der nächste Benutzer, der sich anmeldet, den Inhalt dieser Datei sehen.

Wichtig: Weisen Sie daher die Benutzer an, grundsätzlich alle sicherheitsrelevanten Anwendungen, die als permanente Prozesse festgelegt sind, zu schließen, bevor sie ihre Hotdesktop-Sitzungen beenden.

Wenn Sie eine Anwendung in der Datei process.xml als permanent definieren und die Anwendung in einem Startskript in session.xml angeben, kann sich die Anzahl der Anwendungsinstanzen erhöhen, wenn die Benutzer neue Anwendungsinstanzen während einer Hotdesktop-Sitzung nicht beenden. Um dies zu verhindern, sollten Sie die Anzahl der Instanzen begrenzen, indem Sie ein Skript oder eine „Wrapper"-Anwendung erstellen, das bzw. die die Anwendung startet. Sie können auch die Anwendung selbst bearbeiten, um sicherzustellen, dass immer nur eine Instanz auf einmal ausgeführt wird.

- Anwendungen, die an der Eingabeaufforderung gestartet werden, werden als Hotdesktop-Konto ausgeführt, selbst wenn sie für die Ausführung als Hotdesktop-Benutzerkonto festgelegt worden sind. Um Anwendungen an der Eingabeaufforderung als Hotdesktop-Benutzerkonto zu starten, müssen Sie die Eingabeaufforderung im Abschnitt <shellexecute_processes> der Datei process.xml angeben. Wenn die Eingabeaufforderung als Hotdesktop-Konto ausgeführt wird, und die Dateitypzuordnung (z. B. *.txt) im Abschnitt <shellexecute_processes> der Datei process.xml definiert ist, wird die Anwendung als Hotdesktop-Benutzerkonto gestartet, wenn der Benutzer eine Datei mit der Dateierweiterung .txt startet.

- Bei permanenten Anwendungen, die das 8.3-Dateiformat verwenden, muss bei der Angabe in process.xml im Pfad der ausführbaren Datei ebenfalls das 8.3-Format verwendet werden.
- Während bei den XML-Tags und den Formatierungen in der Datei process.xml die Groß- bzw. Kleinschreibung berücksichtigt wird, spielt sie bei den Pfadangaben und den Namen der ausführbaren Dateien keine Rolle.
- Wenn Benutzer SAP Logon for Windows (saplogon.exe) ausführen, muss sie als Hotdesktop-Benutzer ausgeführt werden. Geben Sie in der Datei process.xml unter dem Tag <shellexecute_processes> den Eintrag saplogon.exe ein. Weitere Informationen finden Sie unter „<shellexecute_processes>“ auf Seite 227.

Die Datei session.xml

Hinweis: Eine Beispieldatei für session.xml finden Sie im Ordner \Support der Password Manager-CD.

Mit der Datei session.xml können Sie die Anwendungen festlegen, die beim Starten einer Hotdesktop-Sitzung gestartet werden (Startskript) und Dateien und andere Informationen entfernen, die nach einer Benutzersitzung noch vorhanden sind (Skript zum Beenden). Bearbeiten Sie die Datei nach Bedarf und speichern Sie sie auf einer Netzwerkfreigabe oder an einem anderen zentralen Speicherort, damit die Hotdesktop-Arbeitsstationen darauf zugreifen können. Legen Sie den Speicherort dieser Datei session.xml in der Benutzerkonfiguration fest. Weitere Informationen finden Sie unter „Einstellungen der Benutzerkonfiguration für Hotdesktop“ auf Seite 229 und „Erweiterte Einstellungen“ auf Seite 122.

Starten von Anwendungen mit der Datei session.xml

Beachten Sie hierbei Folgendes:

- Die Anwendungen, die Sie in der Datei session.xml angeben, müssen bereits auf der Arbeitsstation installiert sein.
- Da Hotdesktop Teil von Password Manager Agent ist, startet der Agent automatisch und muss nicht in dieser Datei angegeben werden.

Andere Anwendungen, die in der Datei session.xml angegeben sind, können unter der Shell des Hotdesktop-Kontos gestartet werden; die Benutzer müssen möglicherweise Anmeldeinformationen eingeben. Die Agentsoftware wird dann gemäß den Einstellungen in den Benutzerkonfigurationen ausgeführt.

Wichtig: Speichern Sie die Datei session.xml im UTF-8-Format. ANSI-Kodierung ist zulässig, wenn alle Zeichen sich im Bereich von 0 bis 127 (Standardzeichensatz für Englisch) befinden. Wenn die Datei session.xml Sonderzeichen oder Zeichen aus anderen Schriftsystemen enthält, wie z. B. asiatische Schriftzeichen, müssen Sie sie im UTF-8-Format speichern.

Tags für session.xml

Die zusätzlichen benutzerdefinierten Tags in der Datei müssen sich zwischen den Tags <session_settings> und </session_settings> in der Datei befinden.

<startup_scripts>

In diesem Dateiabschnitt werden alle Anwendungen angegeben, die unter dem Hotdesktop-Konto und dem Windows-Konto für den Hotdesktop-Benutzer gestartet werden.

```
<startup_scripts>

    <skript>

        <account>Konto<account>

        <working_directory>Arbeitsverzeichnis<working_directory>

        <path>Pfadoptionen</path>

    </script>

</startup_scripts>
```

Wobei Folgendes gilt:

Konto	Gibt das Konto an, unter dem die Anwendung ausgeführt wird. Zur Verfügung stehen **Hotdesktop-Benutzer** oder der Benutzername für das Hotdesktop-Konto.
Arbeitsverzeichnis	Gibt das Arbeitsverzeichnis der Anwendung an.
Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen PC an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: `c:\Programme\InternetExplorer\iexplore.exe http://www.yahoo.com`

<shutdown_scripts>

Bearbeiten Sie in der Datei session.xml die Anwendungen zum Beenden von Hotdesktop, damit alle nicht verwendeten Daten aus der vorherigen Benutzersitzung entfernt werden. In der Regel werden von diesen Anwendungen die Konfigurationsdateien entfernt, die den nächsten Benutzer am Arbeiten hindern könnten, sowie sicherheitsrelevante Dateien, wie z. B. Protokolle, und im System gespeicherte Dokumente. Diese Anwendungen sollten sicherstellen, dass die Hotdesktop-Umgebung für die nächste Benutzersitzung bereinigt ist. Dieser Teil der Datei ist speziell für die Datensicherheit wichtig.

Hinweis: Bei Bedarf können Sie Administratorprogramme oder Skripte initiieren, mit denen die Benutzerumgebung nach dem Abmelden bereinigt wird. So können Sie z. B. mit der Drittanbieteranwendung ein Visual Basic-Skript schreiben, mit dem benutzerspezifische INI-Dateien gelöscht werden.

```
<shutdown_scripts>
    <skript>
        <account>Konto<account>
        <working_directory>Arbeitsverzeichnis<working_directory>
        <path>Pfadoptionen</path>
    </script>
</shutdown_scripts>
```

Wobei Folgendes gilt:

Konto	Gibt das Konto an, unter dem die Anwendung zum Beenden ausgeführt werden soll. Zur Verfügung stehen **Hotdesktop-Benutzer** und der Benutzername für das Hotdesktop-Freigabekonto.
Arbeitsverzeichnis	Gibt das Arbeitsverzeichnis der Anwendung an.
Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen PC an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: `c:\cleanup.vbs`

Beispiel: Starten von Internet Explorer

Starten Sie Internet Explorer mit der URL des firmeninternen Intranets (mycompany.com). In diesem Fall wird Internet Explorer als Prozess ausgeführt, der dem Hotdesktop-Benutzer zugeordnet ist.

Die zusätzlichen benutzerdefinierten Tags in der Datei müssen sich zwischen den Tags <session_settings> und </session_settings> in der Datei befinden.

```
<startup_scripts>

    <skript>

        <account>Hotdesktop-Benutzer</account>

        <Arbeitsverzeichnis>c:\Programme\Internet 
Explorer</Arbeitsverzeichnis>

        <path>c:\Programme\Internet Explorer\iexplore.exe 
http://www.mycompany.com</path>

    </script>

</startup_scripts>
```

Beispiel: Bereinigen einer Sitzung mit einem Skript

Verwenden Sie ein mit Visual Basic erstelltes Skript zum Beenden, um alle Benutzerdaten zu bereinigen, die am Ende einer Sitzung noch vorhanden sind. Das Skript session_cleanup.vbs wird als Hotdesktop-Konto (mit der Bezeichnung HDSA) gestartet und befindet sich unter C:\.

```
<shutdown_scripts>
    <skript>
        <account>HDSA</account>
        <Arbeitsverzeichnis>c:\</Arbeitsverzeichnis>
        <Pfad>c:\session_cleanup.vbs</Pfad>
    </script>
</shutdown_scripts>
```

Die Datei process.xml

Hinweis: Die Datei process.xml wird auf allen Arbeitsstationen oder Geräten erstellt, auf denen Hotdesktop im Verzeichnis C:\Programme\Citrix\MetaFrame Password Manager\HotDesktop installiert ist. Eine Beispieldatei für process.xml finden Sie auch im Ordner \Support der Password Manager-CD. Änderungen an dieser Datei müssen daher auf jedem einzelnen Gerät vorgenommen werden. Sie können jedoch über Active Directory jede Datei process.xml für die einzelnen Benutzer über eine Computer-Gruppenrichtlinie ersetzen. Weitere Informationen finden Sie im Citrix Support-Artikel http://support.citrix.com/article/CTX110394.

Legen Sie mit der Datei process.xml fest, welche Anwendungen weiter ausgeführt werden sollen, nachdem sich ein Hotdesktop-Benutzer abgemeldet hat. Diese Anwendungen werden als *permanente Anwendungen* oder *permanente Prozesse* bezeichnet.

Sie können über die Datei process.xml auch alle Anwendungen festlegen, die nach dem Abmelden eines Hotdesktop-Benutzers beendet werden. Diese Anwendungen werden als *temporäre Anwendungen* oder *temporäre Prozesse* bezeichnet.

Wichtig: Speichern Sie die Datei process.xml im UTF-8-Format. ANSI-Kodierung ist zulässig, wenn alle Zeichen sich im Bereich von 0 bis 127 (Standardzeichensatz für Englisch) befinden. Wenn die Datei process.xml Sonderzeichen oder Zeichen aus anderen Schriftsystemen enthält, wie z. B. asiatische Schriftzeichen, müssen Sie sie im UTF-8-Format speichern.

Tags für process.xml

Die zusätzlichen benutzerdefinierten Tags in der Datei müssen sich zwischen den Tags <configuration> und </configuration> in der Datei befinden.

<persistent_processes>

In diesem Dateiabschnitt können Sie alle Anwendungen angeben, die weiter ausgeführt werden, nachdem sich der Hotdesktop-Benutzer abgemeldet hat. Angegebene Anwendungen werden nach dem Beenden (Abmelden) der Hotdesktop-Sitzungen nicht geschlossen, selbst wenn sie während einer Sitzung gestartet wurden. Geben Sie den vollständigen Pfad des permanenten Prozesses an, um sicherzustellen, dass nur die gewünschten Prozesse nach jeder Sitzung weiter ausgeführt werden.

```
<persistent_processes>
    <process>
        <name>Pfadoptionen</name>
    </process>
</persistent_processes>
```

Wobei Folgendes gilt:

Pfadoptionen	Gibt den vollqualifizierten Ordnerpfad für die ausführbare Datei der Anwendung oder das Skript auf dem lokalen PC an sowie alle Optionen, die mit der Anwendung auszuführen sind. Beispiel: `c:\Programme\Internet Explorer\iexplore.exe. http://www.yahoo.com`

Hinweis: Nach der Installation wird von der Agentsoftware in der Datei process.xml automatisch ein Eintrag für eine permanente Anwendung namens activator.exe erstellt. Die Anwendung activator.exe ruft die Hotdesktop-Sitzungsanzeige für Benutzer auf. Die Sitzungsanzeige ist ein transparentes verschiebbares Fenster, das die Benutzer beim Anmelden sehen. Es enthält vom Administrator definierte Informationen zu Benutzern und ihren Sitzungen. Activator.exe gehört standardmäßig zu den permanenten Prozessen, d. h., die Anwendung wird nicht neu gestartet, wenn sich einer der Hotdesktop-Benutzer an- oder abmeldet.

<transient_processes>

Hinweis: Nach der Installation wird von der Agentsoftware in der Datei process.xml automatisch eine temporäre Anwendung namens shellexecute.exe festgelegt. Die Anwendung ist standardmäßig als temporärer Prozess definiert und wird beendet, wenn sich einer der Hotdesktop-Benutzer abmeldet.

In diesem Dateiabschnitt können Sie alle Anwendungen angeben, die beendet werden, nachdem sich der Hotdesktop-Benutzer abgemeldet hat.

```
<transient_processes>
    <process>
        <name>Anwendungsname</name>
    </process>
</transient_processes>
```

Wobei Folgendes gilt:

Anwendungsname	Gibt nur den Anwendungsnamen des Prozesses oder der Anwendung an, der bzw. die beendet wird. Der vollständige Pfad ist nicht erforderlich. Beispiel: `pnagent.exe`.

<shellexecute_processes>

Hinweis: Nach der Installation wird von der Agentsoftware in der Datei process.xml automatisch eine ausführbare Shell-Anwendung namens ssoshell.exe (Password Manager Agent) festgelegt. Standardmäßig ist dies der Prozess, der als Hotdesktop-Benutzer ausgeführt wird.

In diesem Dateiabschnitt können Sie alle Anwendungen oder Dateitypen angeben, die als Hotdesktop-Benutzer ausgeführt werden. Diese Einstellung gewährleistet die Sicherheit der Anwendungen, die mit den Anmeldeinformationen der aktuell angemeldeten Benutzer ausgeführt werden. Sie können beispielsweise Program Neighborhood Agent angeben, damit das Programm beim Start mit den Anmeldeinformationen des Benutzers ausgeführt wird.

Während im Startskript in der Datei session.xml die Anwendungen festgelegt sind, die beim Starten einer Hotdesktop-Sitzung gestartet werden, werden in <shellexecute_processes> die Anwendungen aufgelistet, die Benutzer im Rahmen einer Hotdesktop-Sitzung starten können.

```
<shellexecute_processes>
    <process>
        <name>Anwendungsname</name>
    </process>
</shellexecute_processes>
```

Wobei Folgendes gilt:

Anwendungsname	Gibt nur den Anwendungsnamen des Prozesses oder der Anwendung an, der bzw. die ausgeführt wird. Der vollständige Pfad ist nicht erforderlich. Beispiel: `pnagent.exe`.

Hinweis: process.xml ermöglicht zusätzlich zu statischen Dateinamen, wie z. B. Notepad.exe, auch die Verwendung von Platzhalterzeichen („*“). Platzhalterzeichen können einzeln oder zusammen mit Dateinamen verwendet werden. Beispiel: Die Namen *.txt, pnagent.exe und *.doc sind gültige Werte für *Anwendungsname*.

Einstellungen der Benutzerkonfiguration für Hotdesktop

Mit den folgenden Einstellungen der Benutzerkonfiguration können Sie die Benutzererfahrung von Hotdesktop weiter anpassen.

Einstellung	Siehe Abschnitt
Skriptpfad für Sitzungseinstellungen	„So legen Sie den Speicherort der Datei session.xml fest“ auf Seite 229
Sperrtimeout	„Festlegen von Timeoutoptionen für Hotdesktop-Sitzungen“ auf Seite 230
Sitzungstimeout	„Festlegen von Timeoutoptionen für Hotdesktop-Sitzungen“ auf Seite 230
Sitzungsanzeige aktivieren	„Aktivieren der Hotdesktop-Sitzungsanzeige“ auf Seite 230
Sitzungsanzeigegrafik	„Festlegen einer benutzerdefinierten Bitmapgrafik als Sitzungsanzeige“ auf Seite 231

Speicherort von Hotdesktop-Einstellungen in einer Benutzerkonfiguration

- Beim Erstellen einer neuen Benutzerkonfiguration sind diese Einstellungen im Dialogfeld **Agentverhalten konfigurieren** unter **Erweiterte Einstellungen** verfügbar.
- Beim Ändern einer vorhandenen Benutzerkonfiguration sind diese Einstellungen im Dialogfeld **Benutzerkonfiguration bearbeiten** im Bereich **Hotdesktop** verfügbar.

Siehe auch „Erstellen von Benutzerkonfigurationen“ auf Seite 107.

So legen Sie den Speicherort der Datei session.xml fest

1. Geben Sie im Textfeld **Skriptpfad für Sitzungseinstellungen** den Speicherort der Datei session.xml ein.

   Dies kann auch ein Netzwerkfreigabeordner ein. Wenn Sie die Datei session.xml zum Beispiel auf einer Netzwerkfreigabe wie \\Citrix\MPM\Share\ speichern, geben Sie hier den zugehörigen Pfad ein.

2. Starten Sie die Hotdesktop-Arbeitsstation nach dem Speichern der Benutzerkonfiguration und Installieren der Datei session.xml neu.

Festlegen von Timeoutoptionen für Hotdesktop-Sitzungen

Mit den Timeoutoptionen können Sie definieren, wie lange Hotdesktop-Sitzungen inaktiv bleiben können, bevor die Arbeitsstation gesperrt oder die Sitzung beendet wird.

- Sitzungstimeout

  Gibt an, wie viele Minuten eine Hotdesktop-Sitzung bei gesperrter Arbeitsstation ausgeführt werden kann. Nach Ablauf des Zeitraums wird die Sitzung beendet, und eine neue Sitzung wird gestartet, wenn die Sperrung des Desktops aufgehoben wird. Der Standardwert ist 5 Minuten.

- Sperrtimeout

  Gibt an, wie viele Minuten eine Hotdesktop-Sitzung aktiv ist, wenn die Arbeitsstation im Leerlauf ist. Nach Ablauf der festgelegten Zeit wird der Desktop gesperrt. Der Standardwert ist 10 Minuten.

Hinweis: Wenn Hotdesktop in der Password Manager-Umgebung gemeinsam mit der Funktion zur automatischen Schlüsselwiederherstellung verwendet wird, werden Kennwortänderungen, die vom Administrator vorgenommen wurden, nicht an die Agentsoftware der betroffenen Benutzer mit aktiven Hotdesktop-Sitzungen weitergegeben.

Wenn diese Benutzer die aktiven Sitzungen sperren und dann versuchen, die Sperrung aufzuheben, werden sie unter Umständen unerwartet zur Eingabe des alten Kennworts aufgefordert. Benutzer sollten das Dialogfeld **Altes Kennwort** schließen und die Hotdesktop-Sitzung durch Abmelden beenden und neu starten, um die Agentsoftware weiterzuverwenden.

Siehe auch „Hotdesktop, Smartcards und Schlüsselwiederherstellung“ auf Seite 216.

Aktivieren der Hotdesktop-Sitzungsanzeige

Wählen Sie die Option **Sitzungsanzeige aktivieren**, damit Benutzer schneller erkennen können, auf welchen Arbeitsstationen Hotdesktop ausgeführt wird. (Die Option ist standardmäßig ausgewählt.) Die Sitzungsanzeige ist ein transparentes verschiebbares Fenster, dass angemeldeten Benutzern angezeigt wird. Die Sitzungsanzeige zeigt den Benutzernamen des Hotdesktop-Benutzers, den Domänennamen, die Benutzerbeschreibung und die Zeit an, zu der sich der Benutzer angemeldet hat. Außerdem kann eine optionale Bitmapgrafik, z. B. ein Firmenlogo, angezeigt werden.

Festlegen einer benutzerdefinierten Bitmapgrafik als Sitzungsanzeige

Wenn Sie eine eigene Bitmapgrafik als Sitzungsanzeige verwenden möchten, können Sie die Grafikdatei auf die einzelnen Hotdesktop-Arbeitsstationen kopieren und den entsprechenden lokalen Grafikpfad angeben oder auf einer Netzwerkfreigabe speichern, auf die alle Hotdesktop-Arbeitsstationen zugreifen können, und einen UNC-Pfad verwenden.

Im Ordner %ProgrammFiles%\Citrix\MetaFrame Password Manager \Hot Desktop steht hierfür auf den einzelnen Hotdesktop-Arbeitsstationen die Standardgrafik Citrix.bmp bereit.

Verwenden des Hotdesktop-Bildschirmschoners

Damit die Benutzer einfacher feststellen können, auf welchen Arbeitsstationen Hotdesktop ausgeführt wird, enthält die Hotdesktop-Installation einen individuell anpassbaren Bildschirmschoner. Der Bildschirmschoner wird erst gestartet, wenn die Arbeitsstation 10 Minuten lang inaktiv war.

Hinweis: Eine gesperrte Sitzung wird als aktive Sitzung betrachtet. Der Bildschirmschoner wird erst gestartet, wenn das Gerät 10 Minuten lang im Leerlauf ist, oder sich alle Benutzer von der Arbeitsstation abgemeldet haben.

Installieren von Hotdesktop

Achtung: Alle Softwarepakete, die die GINA-Kette ändern, z. B. Software zur Unterstützung von Authentifizierungsgeräten, müssen vor Hotdesktop installiert werden. Weitere Informationen finden Sie unter „Erhalten der GINA-Kette bei der Agentinstallation“ im *Citrix Password Manager-Installationshandbuch*.

Hotdesktop ist eine optionale Funktion der Agentsoftware. Weitere Informationen finden Sie unter „Installieren und Konfigurieren von Password Manager Agent“ im *Citrix Password Manager-Installationshandbuch*.

In diesem Abschnitt werden die folgenden Themen beschrieben:

- „So installieren Sie Hotdesktop (neue Agentinstallation)“ auf Seite 233
- „So installieren Sie Hotdesktop (bestehende Agentinstallation)“ auf Seite 233
- „Deaktivieren der Terminaldienste für eine administrative Installation bzw. Installation ohne Benutzereingriffe von Hotdesktop“ auf Seite 232

Hinweis: Hotdesktop wird nur unter Microsoft Windows 2000 Professional, Microsoft Windows XP Embedded und Microsoft Windows XP Professional, Service Pack 2 (32 Bit) unterstützt. Die Funktion wird nicht unter 64-Bit-Betriebssystemen oder Serverbetriebssystemen unterstützt.

Deaktivieren der Terminaldienste für eine administrative Installation bzw. Installation ohne Benutzereingriffe von Hotdesktop

Damit Hotdesktop korrekt installiert wird, müssen die Terminaldienste deaktiviert werden. Wenn Sie ein Microsoft Windows Installer-Paket (.msi) für eine administrative Hotdesktop-Installation oder eine Hotdesktop-Installation ohne Benutzereingriffe erstellen, müssen Sie die Eigenschaft `DISABLE_TERMINAL_SERVICE` auf 1 einstellen, bevor Sie Hotdesktop auf den Arbeitsstationen installieren. Weitere Informationen finden Sie unter „Installieren und Konfigurieren von Password Manager Agent“ im *Citrix Password Manager-Installationshandbuch*.

Sie können auch eine Transformation erstellen, die den Eigenschaftswert für Pakete festlegt, die durch die Active Directory-Gruppenrichtlinie automatisch bereitgestellt werden.

So installieren Sie Hotdesktop (neue Agentinstallation)

Weitere Informationen finden Sie unter „Installieren und Konfigurieren von Password Manager Agent“ im *Citrix Password Manager-Installationshandbuch*.

So installieren Sie Hotdesktop (bestehende Agentinstallation)

1. Melden Sie sich an der Arbeitsstation als lokaler Administrator an.
2. Wählen Sie in der Systemsteuerung **Software**.
3. Wählen Sie **Citrix Password Manager Agent** und klicken Sie auf **Ändern**.
4. Wählen Sie die Option **Ändern** und klicken Sie auf **Weiter**.
5. Wählen Sie die Option **Hotdesktop** und klicken Sie auf **Weiter**.
6. Bestätigen Sie die Meldung mit **Ja**, um Terminaldienste und Remotedesktop zu deaktivieren.
7. Geben Sie den Speicherort des zentralen Speichers an und klicken Sie auf **Weiter**.
8. Geben Sie die Adresse des Dienstservers ein und klicken Sie auf **Weiter**.
9. Geben Sie die Anmeldeinformationen des Benutzers für das Hotdesktop-Konto ein und klicken Sie auf **Weiter**.

   Geben Sie den Namen der Domäne an, zu der die Arbeitsstation gehört. Verwenden Sie dabei den NetBIOS-Namen der Domäne und nicht den vollqualifizierten Domänennamen.
10. Klicken Sie auf **Installieren**.

    Klicken Sie auf **Zurück**, wenn Sie eine Einstellung oder Auswahl ändern möchten.
11. Legen Sie die Produkt-CD ins CD-ROM-Laufwerk ein, um die Agentdatei setup.msi bereitzustellen.
12. Klicken Sie auf **Fertig stellen**, um die Installation abzuschließen.
13. Bestätigen Sie den Neustart des Clientgeräts mit **Ja**.

Deinstallieren von Hotdesktop

Wenn Sie die Hotdesktop-Funktion von einer Arbeitsstation entfernen müssen, führen Sie die Schritte unter „So deinstallieren Sie Hotdesktop“ auf Seite 234 aus.

Möglicherweise müssen Sie nach der Deinstallation der Hotdesktop-Funktion auch folgende Schritte ausführen:

- „Wiederherstellen von Terminaldiensten nach dem Deinstallieren von Hotdesktop“ auf Seite 236
- „Aktivieren mehrerer Sitzungen nach dem Deinstallieren von Hotdesktop“ auf Seite 237

Achtung: Im Rahmen dieses Verfahrens müssen Sie die Registrierung bearbeiten. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Verwenden Sie den Registrierungs-Editor auf eigene Verantwortung. Legen Sie stets eine Sicherungskopie der Systemregistrierung an, bevor Sie fortfahren.

So deinstallieren Sie Hotdesktop

1. Halten Sie während des Windows-Startvorgangs die Umschalttaste gedrückt, um sich an der freigegebenen Arbeitsstation oder dem Clientgerät anzumelden und Administratoraufgaben auszuführen.

   Damit verhindern Sie, dass das Hotdesktop-Konto angemeldet wird und die Hotdesktop-Umgebung startet. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.

   Melden Sie sich als Administrator an.
2. Öffnen Sie die Systemsteuerung und wählen Sie **Software**.
3. Wählen Sie **Citrix Password Manager Agent**.
4. Klicken Sie auf **Ändern**, um nur die Funktion **Hotdesktop** zu entfernen.

5. Klicken Sie im Dialogfeld **Anwendungswartung** auf **Ändern**.
6. Klicken Sie im Dialogfeld **Funktionsauswahl** auf **Hotdesktop** und deaktivieren Sie die Funktion.
7. Wählen Sie den Typ des zentralen Speichers und bestätigen Sie die Änderungen an der Agentsoftware.
8. Starten Sie die Arbeitsstation neu.

Hotdesktop ist erst nach dem Neustart der Arbeitsstation komplett entfernt.

Wichtig: Beim Deinstallieren von Software, die die GINA-Kette unterbrochen haben könnte, ist es wichtig, die Software auf dem Clientgerät in der umgekehrten Reihenfolge zur Installation zu deinstallieren. Wenn dies nicht beachtet wird, kann es passieren, dass der Computer nicht mehr funktionsfähig ist. Bearbeiten Sie nicht die Registrierung. Weitere Informationen finden Sie unter „Erhalten der GINA-Kette bei der Agentinstallation“ im *Citrix Password Manager-Installationshandbuch*.

Wiederherstellen von Terminaldiensten nach dem Deinstallieren von Hotdesktop

Achtung: Im Rahmen dieses Verfahrens müssen Sie die Registrierung bearbeiten. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Verwenden Sie den Registrierungs-Editor auf eigenes Risiko. Legen Sie stets eine Sicherungskopie der Systemregistrierung an, bevor Sie fortfahren.

Der Hotdesktop-Installationsprozess deaktiviert die Terminaldienste. Führen Sie die folgenden Schritte aus, um die Terminaldienste zu aktivieren.

So aktivieren Sie die Terminaldienste nach der Deinstallation von Hotdesktop

1. Melden Sie sich an der Arbeitsstation als Administrator an.
2. Klicken Sie auf **Start > Ausführen** und geben Sie **regedit** ein.
3. Legen Sie für den Registrierungsschlüssel gemäß folgender Angabe den Wert **1** fest:

   [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
   \Control\Terminal Server]TSEnabled=dword:00000001

Aktivieren mehrerer Sitzungen nach dem Deinstallieren von Hotdesktop

Achtung: Im Rahmen dieses Verfahrens müssen Sie die Registrierung bearbeiten. Die unsachgemäße Verwendung des Registrierungs-Editors kann zu schwerwiegenden Problemen führen, die möglicherweise nur durch Neuinstallation des Betriebssystems gelöst werden können. Citrix übernimmt keine Garantie dafür, dass Probleme, die auf eine unsachgemäße Verwendung des Registrierungs-Editors zurückzuführen sind, behoben werden können. Verwenden Sie den Registrierungs-Editor auf eigenes Risiko. Legen Sie stets eine Sicherungskopie der Systemregistrierung an, bevor Sie fortfahren.

Während der Hotdesktop-Installation setzt das Installationsprogramm diesen Registrierungsschlüssel auf 0 zurück. Führen Sie folgende Schritte durch, um mehrere Sitzungen zu aktivieren.

So aktivieren Sie mehrere Sitzungen

1. Melden Sie sich an der Arbeitsstation als Administrator an.
2. Klicken Sie auf **Start** > **Ausführen** und geben Sie **regedit** ein.
3. Ändern Sie den Wert des Registrierungsschlüssels zu **1**:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT \Current Version\Winlogon] AllowMultipleSessions =dword:00000001

Zusammenwirken mit Citrix Presentation Server Clients

Password Manager unterstützt die Verwendung von Citrix Presentation Server Client-Paketen mit Hotdesktop. In diesem Abschnitt finden Sie einige allgemeine Richtlinien für die Verwendung von Hotdesktop mit Presentation Server Clients, wie Program Neighborhood Agent und dem Webinterface:

- Bearbeiten Sie die Datei process.xml, um die Presentation Server Clients als temporäre Prozesse festzulegen (falls der Client vom Windows-Startprogramm gestartet wird, und bereits beim Start der ersten Hotdesktop-Sitzung ausgeführt werden).
- Wenn Sie Security Service Provider Interface verwenden, müssen Sie den Client als Hotdesktop-Benutzer ausführen. Sie können den Client auch als Hotdesktop-Benutzer ausführen, wenn Sie Sicherheitsbedenken haben. Die ICA-Dateien werden im Profil gespeichert.
    - Bearbeiten Sie den Abschnitt <shellexecute_processes> der Datei process.xml so, dass die Clients von der Windows-Shell aus als Hotdesktop-Benutzerkonten gestartet werden.
    - Bearbeiten Sie die Datei session.xml, um ein Startskript oder eine ausführbare Datei festzulegen, das bzw. die beim Start der ersten Hotdesktop-Sitzung auch den Client startet.

Program Neighborhood Agent

Sie können Program Neighborhood Agent für SSPI (Security Service Provider Interface) konfigurieren. Mit Security Service Provider Interface kann sich Program Neighborhood Agent als Hotdesktop-Benutzer am Server mit Presentation Server authentifizieren. Stellen Sie sicher, dass Presentation Server der Windows-Sicherheitsautorität vertraut, die für die Authentifizierung des Hotdesktop-Benutzers verwendet wird. Weitere Informationen zur Konfiguration von Security Service Provider Interface für Program Neighborhood Agent finden Sie im *Citrix Presentation Server-Administratorhandbuch*.

Citrix Webinterface

In einer Presentation Server-Umgebung kann der Hotdesktop-Agent Anmeldeinformationen über den Webinterface Client senden. Weitere Informationen zum Konfigurieren des Webinterface finden Sie im *Webinterface-Administratorhandbuch*.

Anzeigen von Hotdesktop-Benutzerprofilen

In einer Hotdesktop-Umgebung wird die Shell (explorer.exe) als Hotdesktop-Konto ausgeführt. Das bedeutet, dass die Shell keine Zugriffsrechte für das Navigieren zum Hotdesktop-Benutzerprofilordner hat.

So zeigen Sie Hotdesktop-Profile an

1. Nehmen Sie in der Datei process.xml unter <shellexecute_processes> Internet Explorer (iexplore.exe) auf, damit diese Anwendung als Hotdesktop-Benutzer ausgeführt wird.
2. Melden Sie sich als Hotdesktop-Benutzer an und starten Sie Internet Explorer.
3. Geben Sie zum Anzeigen der Profile in der Adressleiste den vollständigen Pfad zum Hotdesktop-Benutzerprofilverzeichnis ein. Beispiel:

   C:\Dokumente und Einstellungen\All Users\Anwendungsdaten \Citrix\MetaFrame Password Manager

Herunterfahren von Hotdesktop-Arbeitsstationen

Da nur Administratoren Hotdesktop-Arbeitsstationen herunterfahren dürfen, enthält das Startmenü von Hotdesktop-Arbeitsstationen keine Option **Beenden**.

Drücken Sie zum Herunterfahren einer Hotdesktop-Arbeitsstation für administrative Zwecke STRG+ALT+ENTF. Klicken Sie dann im Dialogfeld **Windows-Sicherheit** auf **Beenden**.

Arbeiten ohne AutoAdminLogon-Unterstützung

Wenn AutoAdminLogon aktiviert ist, kann es passieren, dass die Authentifizierung mit Drittanbieterprodukten nicht funktioniert. Einige Drittanbieteranwendungen deaktivieren oder entfernen den AutoAdminLogon-Wert während der Installation. In dieser Situation müssen Sie AutoAdminLogon von Hotdesktop mit den folgenden Schritten deaktivieren:

1. Starten Sie die freigegebene Arbeitsstation oder das Clientgerät neu und halten Sie während des Windows-Startvorgangs die **Umschalttaste** gedrückt.

   Damit verhindern Sie, dass das Hotdesktop-Konto angemeldet wird und die Hotdesktop-Umgebung startet. Weitere Informationen zum Umgehen der automatischen Windows-Anmeldung finden Sie auf der Website von Microsoft.

2. Melden Sie sich als Administrator an.

3. Bearbeiten Sie die Registrierung und legen Sie unter HKEY_LOCAL_MACHINE\SOFTWARE\Citrix \MetaFrame Password Manager\HotDesktop die folgenden Werte fest:

Wertname	Typ	Wert
AutoAdminLogon	REG_SZ	0 zum Deaktivieren

4. Starten Sie nach dem Festlegen des Wertes die Arbeitsstation neu und melden Sie sich manuell mit den Anmeldeinformationen für das Hotdesktop-Konto an. Die Hotdesktop-Anmeldeseite wird angezeigt, von der aus die Benutzer eine Authentifizierung mit einer Drittanbieteranwendung durchführen können.

Ändern des Kennworts für das Hotdesktop-Konto

Unter Umständen müssen Sie das Kennwort für das Hotdesktop-Konto ändern. Sie haben die Anmeldeinformationen des Kontos bei der Agentinstallation eingegeben. Mit der folgenden Vorgehensweise können Sie das Kennwort ändern.

So ändern Sie das Kennwort für das Hotdesktop-Konto

1. Melden Sie sich an einer Arbeitsstation an, auf der Hotdesktop installiert ist.

Wichtig: Verwenden Sie für Schritt 1 weder ein Administratorkonto noch die Anmeldeinformationen für das Hotdesktop-Konto.

---

2. Drücken Sie die Tastenkombination Strg+Alt+Entf, um das Dialogfeld **Windows-Sicherheit** anzuzeigen.
3. Klicken Sie auf **Kennwort ändern**.
4. Geben Sie Folgendes ein oder wählen Sie einen Eintrag aus:
   - Benutzername für das Hotdesktop-Konto
   - Domänenname oder Name des lokalen Computers
   - Altes Kennwort
   - Neues Kennwort
5. Klicken Sie auf **OK**.
6. Klicken Sie auf **Herunterfahren** und dann im Dialogfeld **Windows-Sicherheit** auf **Neu starten**, um den PC neu zu starten.

Informationen zu Hotdesktop im Web

Weitere Informationen zu Hotdesktop finden Sie im folgenden Artikel im Citrix Knowledge Center:

- http://support.citrix.com/article/CTX108740, *Hot Desktop FAQ*
- http://support.citrix.com/article/CTX108771, *Hot Desktop Shared AccountUpdate Tool*
- http://support.citrix.com/article/CTX110394, *Replacing Users' Process.xml File in Hot Desktop Through a Machine Group Policy*

Vorgänge

In diesem Kapitel finden Sie Informationen zum Beheben von Problemen bei der Installation von Password Manager sowie zusätzliche Informationen zu bestimmten Funktionen und Merkmalen von Password Manager. Die besten Installationsergebnisse erzielen Sie, wenn Sie die in den anderen Abschnitten dieses Handbuchs genannten Verfahren zum Konfigurieren von Password Manager einhalten.

Dieses Kapitel enthält Informationen zu den folgenden Themen:

Aufzeichnen von Password Manager-Ereignissen

Password Manager Agent kann agent- oder benutzergenerierte Ereignisse im Windows-Ereignisprotokoll der Anwendung auf dem Hostcomputer aufzeichnen. Die Ereignisse werden dabei als Informationen, Warnung oder Fehler klassifiziert.

Im Ereignisprotokoll werden sicherheitsrelevante Ereignisse erfasst und verifiziert, die u. U. aufgrund gesetzlicher oder regulatorischer Auflagen aufgezeichnet und aufbewahrt werden müssen. Die Möglichkeiten der Ereignisprotokollierung in Password Manager helfen Ihnen auch, Ihre IT-Sicherheit zu erhöhen.

Wenn Sie Password Manager in einer Presentation Server-Umgebung verwenden, enthält das Ereignisprotokoll sowohl Benutzer- als auch Sitzungsinformationen. Es werden sämtliche fehlgeschlagenen Anmeldeversuche erfasst.

Die Standardprotokollierung ist zwar standardmäßig deaktiviert, Sie können das Ereignisprotokoll aber in der Konsole aktivieren, nachdem Sie die Benutzerkonfiguration erstellt haben. Die Hotdesktop-Ereignisprotokollierung ist immer aktiviert. Password Manager zeichnet Ereignisse z. B. für die folgenden Funktionen auf:

- Hotdesktop (standardmäßig aktiviert)
- Smartcards
- Lizenzierung
- Password Manager-Dienst

In der folgenden Tabelle finden Sie eine Übersicht über einige der Standardereignisse, die von Password Manager aufgezeichnet werden:

Standardereignistypen
Anmeldeversuch fehlgeschlagen (Agentauthentifizierung) Wird aufgezeichnet, wenn ein Benutzer sich nicht erfolgreich an Password Manager Agent authentifizieren kann. Fehler beim Öffnen des Speichers für Anmeldeinformationen.
Anmeldeversuch erfolgreich (Agentauthentifizierung) Wird aufgezeichnet, wenn ein Benutzer sich erfolgreich authentifiziert und den zentralen Speicher öffnen kann.
Anmeldeversuch (Senden von Anmeldeinformationen) Wird aufgezeichnet, wenn versucht wird, Anmeldeinformationen an eine externe Anwendung zu senden.
Vorgänge mit Anmeldeinformationen Wird bei Vorgängen mit Kennwörtern, wie Kennwortänderung, Kennwortanzeige und Identitätsprüfung, aufgezeichnet.
Synchronisierung fehlgeschlagen (Kommunikation) Wird aufgezeichnet, wenn das Synchronisieren mit dem zentralen Speicher aufgrund von Kommunikationsproblemen fehlschlägt.
Synchronisierung fehlgeschlagen (Berechtigungen) Wird aufgezeichnet, wenn das Synchronisieren mit dem zentralen Speicher aufgrund falscher Benutzeranmeldeinformationen fehlschlägt.
Fehler bei Smartcard-DataProtect-Verschlüsselung/-Entschlüsselung Wird aufgezeichnet, wenn es beim Verschlüsseln oder Entschlüsseln von Smartcard-Daten zu einem allgemeinen Fehler kommt.
Fehler bei Smartcard-DataProtect-Verschlüsselung/-Entschlüsselung (Karte fehlt) Wird aufgezeichnet, wenn die Smartcard nicht verfügbar ist.
Starten und Herunterfahren der Agentsoftware Wird aufgezeichnet, wenn die Smartcard nicht verfügbar ist.
Fehlende oder zerstörte DLL-Dateien Wird aufgezeichnet, wenn eine DLL-Datei nicht korrekt geladen werden kann.

In der folgenden Tabelle finden Sie einige der Hotdesktop-Ereignisse, die von Password Manager aufgezeichnet werden.

Hotdesktop-Ereignistypen
Fehler bei der Anmeldung an der Hotdesktop-Sitzung Wird aufgezeichnet, wenn es beim Sitzungsstart zu einem schwerwiegenden Fehler kommt.
Anmeldung an der Hotdesktop-Sitzung erfolgreich Wird aufgezeichnet, wenn Hotdesktop nach erfolgreicher Benutzerauthentifizierung eine Sitzung startet.
Abmelden von Hotdesktop-Sitzung fehlgeschlagen Wird nur aufgezeichnet, wenn es beim Beenden der Sitzung zu einem schwerwiegenden Fehler kommt.
Abmelden von Hotdesktop erfolgreich Wird aufgezeichnet, wenn eine Sitzung infolge einer Benutzereingabe oder eines Sitzungstimeouts erfolgreich beendet wird.

Aktivieren der Ereignisprotokollierung

Gehen Sie zum Aktivieren der Ereignisprotokollierung wie folgt vor:

1. Gehen Sie in der Konsole zur entsprechenden Benutzerkonfiguration und wählen Sie **Benutzerkonfiguration bearbeiten**.
2. Wählen Sie in den Eigenschaften der Benutzerkonfiguration **Clientseitiges Verhalten**.
3. Klicken Sie auf **Citrix Password Manager-Ereignisse mit der Windows-Ereignisprotokollierung aufzeichnen**.

INI-Dateien für die Anwendungserkennung

In Password Manager gibt es vier INI-Dateien mit Anwendungsdefinitionen. Die in der folgenden Tabelle aufgeführten INI-Dateien enthalten Anwendungsdefinitionen, die Password Manager Agent zum Identifizieren und Beantworten von Anforderungen zur Bereitstellung von Anmeldeinformationen verwendet.

Dateiname	Speicherort	Beschreibung
Applist.ini	%ProgramFiles%\Citrix \MetaFrame Password Manager\Plugin\LogonMgr\	Enthält Anwendungsdefinitionen, die nur lokal für diesen Client gültig sind.
Entlist.ini	%AppData%\Citrix\MetaFrame Password Manager\	Enthält Anwendungsdefinitionen, die für das gesamte Unternehmen gültig sind und genutzt werden können. Download vom Synchronisierungspunkt erfolgt automatisch durch die Agentsoftware.
Aelist.ini	%AppData%\Citrix\MetaFrame Password Manager\	Enthält alle Informationen aus den Dateien Applist.ini und Entlist.ini. Wird von Password Manager Agent zum Identifizieren von Anwendungen verwendet. Die Datei aelist.ini wird bei jeder Synchronisierung aus den Dateien Applist.ini und Entlist.ini erstellt.
Mfrmlist.ini	%ProgramFiles%\Citrix \MetaFrame Password Manager\Helper\MFEmu	Enthält eine Liste der Terminalemulatoren und Speicherorte der HLLAPI-DLL, die von Password Manager Agent überwacht wird.

Kein Senden von Anmeldeinformationen von Seiten der Password Manager Agent-Software

Manchmal sendet Password Manager Agent nicht die Anmeldeinformationen eines Benutzers an eine konfigurierte Anwendung. Dieses Problem ist in der Regel auf einen Fehler in der Anwendungsdefinition zurückzuführen. In diesem Abschnitt werden Hinweise zur Behandlung von Anwendungserkennungsproblemen gegeben.

Führen Sie zunächst die folgenden Schritte aus, um die Ursache für das fehlgeschlagene Senden der Anmeldeinformationen zu ermitteln:

- Suchen Sie nach potenziellen Konflikten in den Einstellungen.
- Prüfen Sie, ob Password Manager Agent so konfiguriert ist, dass Anwendungen erkannt werden können.
- Vergleichen Sie die Definitionen von Password Manager Agent mit denen der Password Manager Console.

Hinweis: Password Manager bietet zahlreiche Einstellungen für das Erstellen bzw. Entwickeln von Anwendungsdefinitionen, Kennwortrichtlinien, Benutzerkonfigurationen und Methoden zur Identitätsprüfung. Es ist möglich, widersprüchliche Einstellungen festzulegen, die u. a. dazu führen können, dass Anmeldeinformationen nicht an eine Anwendung gesendet werden. Weitere Informationen finden Sie unter „Liste der Password Manager-Einstellungen“ auf Seite 275.

Wenn Password Manager Agent auch nach dem Ausführen dieser Schritte die Anmeldeinformationen des Benutzers nicht sendet, probieren Sie die nachstehenden Methoden zur Problembehandlung bei Windows-basierten, webbasierten und Terminalemulator-basierten Anwendungen aus.

Alle Formate (Windows, Web, Terminalemulatoren)

So vergewissern Sie sich, dass die Anwendungsdefinition der Konsole mit der Anwendungsdefinition des Clients übereinstimmt

Erstellen Sie in der Konsole Anwendungsdefinitionen für Anwendungen, die mehr als zwei Anmeldeinformationen-Felder (Benutzername und Kennwort) haben, und stellen Sie dann Password Manager Agent die Anwendungsdefinitionen bereit. Sie können überprüfen, ob die Definitionen erfolgreich bereitgestellt wurden, indem Sie die Übereinstimmung der Eigenschaften der Anwendungsdefinitionen der Konsole mit denen auf dem Clientcomputer bestätigen.

1. Klicken Sie auf das Password Manager Agent-Symbol im Infobereich und wählen Sie **Anmeldungsmanager**.
2. Klicken Sie im Menü **Ansicht** auf **Aktualisieren**.
3. Überprüfen Sie auf dem Computer, auf dem Password Manager Agent ausgeführt wird, mit Windows Explorer, ob die Dateien entlist.ini, aelist.ini und ftulist.ini aktualisiert wurden.

   Datum und Uhrzeit der Änderung dieser Dateien müssen mit dem Datum und der Uhrzeit der Dateiaktualisierung übereinstimmen.
4. Falls die Dateien entlist.ini, aelist.ini und ftulist.ini nicht aktualisiert wurden, löschen Sie sie.
5. Gehen Sie zum **Anmeldungsmanager** zurück und klicken Sie im Menü **Ansicht** auf **Aktualisieren**.
6. Vergewissern Sie sich, dass die Dateien wiederhergestellt sind.

Windows-basierte Anwendungen

Erstellen Sie die Anwendungsdefinition in einer Konsole, die auf demselben Betriebssystem läuft, auf dem auch Password Manager Agent ausgeführt wird. Die verschiedenen Windows-Plattformen erkennen Anwendungen u. U. unterschiedlich, was zum Erstellen unterschiedlicher Definitionen für ein und dieselbe Anwendung führt.

So überprüfen Sie den Anwendungspfad und die Fenstertiteldefinitionen

1. Öffnen Sie auf dem Computer, auf dem Password Manager Agent ausgeführt wird, die Datei entlist.ini und überprüfen Sie die Einträge **AppPathKey[n]** und **WindowTitle[n]**.
2. Starten Sie die Anwendung.
3. Vergewissern Sie sich, dass der Anwendungspfad und die Fenstertitel mit den Angaben in der Datei entlist.ini übereinstimmen.
4. Öffnen Sie auf dem Computer, auf dem Password Manager Agent ausgeführt wird, die Datei aelist.ini und vergewissern Sie sich, dass die Einträge **AppPathKey[n]** und **WindowTitle[n]** mit den Einträgen in der Datei entlist.ini übereinstimmen.
5. Stellen Sie sicher, dass jedes Formular nur einen Eintrag in der Datei aelist.ini hat.

   Beim Lesen der Datei aelist.ini verwendet das System die erste Formulardefinition, die mit den Kriterien übereinstimmt. Die Einträge in der Datei aelist.ini werden in einer beliebigen Reihenfolge in die Datei geschrieben, sodass eine Formulardefinition, die als Ersatz hinzugefügt wird, auch an eine Position hinter der ursprünglichen Definition geschrieben werden kann, ohne dass dabei die ursprüngliche Definition ersetzt wird. Das führt dazu, dass das System weiterhin die ursprüngliche Definition verwendet, auch wenn die neue Definition in der Datei vorhanden ist. Wenn Sie mehrere Einträge für dasselbe Formular finden, löschen Sie mit der Konsole die Einträge, die nicht benötigt werden.

So vergewissern Sie sich, dass die Klassen-ID nicht in der Liste der für die Formulare dieser Anwendung zu ignorierenden Fensterklassen aufgeführt ist:

1. Erweitern Sie in der Konsole den Knoten **Anwendungsdefinitionen** und wählen Sie die gewünschte Anwendung aus.
2. Klicken Sie im Menü **Aktion** auf **Anwendungsdefinition bearbeiten**.
3. Klicken Sie auf **Anwendungsformulare**.
4. Wählen Sie aus der Liste **Definierte Anwendungsformulare** ein Anwendungsformular aus und klicken Sie dann auf **Bearbeiten**.

   Das Dialogfeld **Anwendungsformular bearbeiten** wird angezeigt.
5. Klicken Sie auf **Formularidentität**.
6. Klicken Sie auf **Erweiterte Zuordnung**.

   Das Dialogfeld **Erweiterte Zuordnung** wird angezeigt.
7. Falls diese Option nicht bereits ausgewählt ist, klicken Sie auf **Klasseninformationen**, um anzuzeigen, welche Fensterklassen von der Agentsoftware ignoriert werden.

Hinweis: Sie können nach allen ignorierten Fensterklassen suchen, indem Sie in der Datei aelist.ini nach der Zeichenfolge „IgnoreClassName=“ suchen.

Webbasierte Anwendungen

Erstellen Sie Webanwendungsdefinitionen mit dem Assistenten für Anwendungs-definitionen und dem Assistenten für Formulardefinitionen. Der Assistent für Formulardefinitionen stellt sicher, dass Password Manager Webseiten mit der richtigen URL konfiguriert (weitergeleitet, unter Beachtung der Groß- und Kleinschreibung usw.). Außerdem verhindert er typografische Fehler.

So vergewissern Sie sich, dass die Einstellung „Strenge URL-Zuordnung“ korrekt verwendet wird

Die Einstellung **Strenge URL-Zuordnung** befindet sich auf der Seite zur Bearbeitung von Webanwendungsformularen in der Konsole.

1. Wählen Sie in der Konsole die Anwendung aus, die Sie anzeigen möchten.
2. Klicken Sie im Menü **Aktion** auf **Anwendungsdefinition bearbeiten**.
3. Klicken Sie auf **Anwendungsformulare**, wählen Sie ein Anwendungsformular aus klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie auf **Formularidentität**.

   Hier können Sie die strenge URL-Zuordnung sowie die Beachtung der Groß-und Kleinschreibung bei URLs aktivieren.
5. Vergewissern Sie sich, dass die Seiten HTML-kompatible Feldtypen verwenden:

   Webanwendungsdefinitionen müssen HTML-kompatible Feldtypen enthalten. Nicht definierte oder benutzerdefinierte Feldtypen werden nicht erkannt.

Terminalemulator-basierte Anwendungen

Erstellen Sie Terminalemulator-basierte Anwendungsdefinitionen mit dem Assistenten für Anwendungsdefinitionen und dem Assistenten für Formulardefinitionen. Wenn Sie einer Benutzerkonfiguration eine Anwendungsdefinition hinzufügen, stellen Sie sicher, dass die Unterstützung für Terminalemulatoren aktiviert ist.

- **Vergewissern Sie sich, dass der Emulator in der Datei Mfrmlist.ini konfiguriert ist.**

  Der Prozess Ssomho.exe, der das Password Manager Agent-Verhalten mit Terminalemulatoren steuert, erkennt nur Emulatoren, die in der Datei Mfrmlist.ini definiert sind. Wenn der HLLAPI-kompatible Emulator nicht in dieser Datei definiert ist, unternimmt der Prozess Ssomho.exe nicht den Versuch, mit dem Emulator zu kommunizieren.

- **Vergewissern Sie sich, dass ein HLLAPI-Kurzname für die Sitzung festgelegt ist.**

  Der Prozess Ssomho.exe verwendet diesen Kurznamen der Sitzung für die Kommunikation mit der HLLAPI-DLL. Ist kein Kurzname der Sitzung vorhanden, wird Ssomho.exe zwar geladen, die Bildschirmaktivität kann jedoch nicht überwacht werden. Konfigurieren Sie den Kurznamen der Sitzung auf dem Emulator im Clientgerät. Weitere Informationen zum Konfigurieren von Emulatoren mit HLLAPI-Unterstützung finden Sie unter „Konfigurieren der HLLAPI-Unterstützung für getestete Emulatoren“ auf Seite 256.

- **Vergewissern Sie sich, dass der Prozess Ssomho.exe ausgeführt wird.**

  Gehen Sie zur Überprüfung, ob Ssomho.exe ausgeführt wird, wie folgt vor:

  A. Öffnen Sie auf dem Computer, auf dem Password Manager Agent ausgeführt wird, den Task-Manager und wählen Sie die Registerkarte **Prozesse**.

  B. Klicken Sie auf die Überschrift **Abbildname**, um die Prozesse nach ihrem Namen zu sortieren.

  C. Prüfen Sie, ob Ssomho.exe in der Liste aufgeführt ist.

  Wenn der Prozess Ssomho.exe nicht in der Liste aufgeführt ist, könnte es sein, dass der Prozess keine HLLAPI-DLLs gefunden hat oder dass er aufgrund von Drittanbieter-HLLAPI-Problemen vorzeitig beendet wurde.

  Hinweis: Auch wenn der Prozess Ssomho.exe in der Liste aufgeführt wird, ist es möglich, dass er nicht erfolgreich mit der HLLAPI.dll kommuniziert. Vergewissern Sie sich, dass der Kurzname für die Sitzung korrekt ist, bevor Sie nach anderen Gründen für das Problem suchen.

- **Testen Sie jeden Emulator einzeln.**

  Wenn Sie mehrere unterstützte Emulatoren auf demselben System installiert haben, versucht Ssomho.exe, mit allen diesen Emulatoren zu kommunizieren. Es kann passieren, dass eine der HLLAPI-DLL-Implementierungen zur Instabilität von Ssomho.exe führt. Testen Sie daher jeden Hostemulator einzeln, indem Sie die anderen Hostemulatoren entfernen oder die Einträge in der Datei Mfrmlist.ini auskommentieren und neu anordnen.

  Auf diese Weise können Sie gut überprüfen, ob der Prozess Ssomho.exe nicht versehentlich eine Verbindung mit einem anderen Emulator als dem herstellt, den Sie gerade auf Fehler untersuchen.

Unterstützen von Terminalemulatoren

In diesem Abschnitt wird beschrieben, wie Sie Password Manager und die Komponenten für Terminalemulatoren konfigurieren. Password Manager unterstützt HLLAPI-kompatible Terminalemulatoren.

Zum Aktivieren der HLLAPI-Unterstützung für alle Terminalemulatoren in Password Manager müssen Sie die Unterstützung für Terminalemulatoren in der Konsole aktivieren.

Wenn die Host-/Mainframeemulatorunterstützung aktiviert ist, startet SSOShell den Prozess Ssomho.exe. Dieser Prozess liest zuerst die in %ProgramFiles%\Citrix\MetaFrame Password Manager\Helper\MFEmu befindliche Datei Mfrmlist.ini, sucht dann nach allen konfigurierten Emulatoren und versucht anschließend, die in der Datei zugeordnete HLLAPI-kompatible DLL-Datei zu laden.

Die Datei Mfrmlist.ini kann zur Aufnahme zusätzlicher HLLAPI-kompatibler Emulatoren erweitert werden.

Der Prozess Ssomho.exe sucht in der Registrierung unter HKEY_LOCAL_MACHINE\SOFTWARE nach dem Speicherort der HLLAPI-kompatiblen DLL-Datei, sofern in der Datei Mfrmlist.ini nichts anderes festgelegt ist.

Einige Emulatoren platzieren den Speicherort unter HKEY_CURRENT_USER. Bei diesen Emulatoren müssen Sie den Speicherort der DLL-Datei mit der expliziten Pfadeinstellung in der Datei mfrmlist.ini manuell angeben.

Konfigurieren der HLLAPI-Unterstützung für getestete Emulatoren

Das Konfigurieren von Password Manager für das Arbeiten mit getesteten Emulatorprogrammen ist ein mehrstufiger Prozess, bei dem die Emulatorsoftware installiert, eine mit Password Manager zu verwendende Emulatorsitzung erstellt und Password Manager mit einer Hostanwendungsdefinition konfiguriert werden muss, die durch Textabgleich eine bestimmte Emulatorsitzung erkennt.

So konfigurieren Sie die Emulatorunterstützung

1. Installieren Sie die Emulatorsoftware und starten Sie den Computer neu.
2. Starten Sie die Emulatorsoftware und erstellen Sie eine neue Sitzung. Definieren Sie dabei die Anzeige und die Verbindung.
3. Legen Sie einen Kurznamen für die Sitzung fest.
4. Aktivieren Sie die HLLAPI-API-Unterstützung.

Hinweis: Für jede einzelne Sitzung, die mit Password Manager verwendet wird, wird eine separate Hostanwendungsdefinition benötigt. Die Agentsoftware erkennt Sitzungen, indem sie Text auf dem Hostanwendungsbildschirm Text in einer bestimmten, von der Anwendungsdefinition vorgegebenen Zeile und Spalte zuordnet. Password Manager Agent sendet dann die in der vorgegebenen Zeile und Spalte der Anwendungsdefinition gefundenen Anmeldeinformationen. Deshalb benötigt jede einzelne Sitzung eine eigene Hostanwendungsdefinition.

---

5. Speichern und schließen Sie die Sitzung.
6. Beenden Sie den Emulator.
7. Erstellen Sie eine Anwendungsdefinition für die Hostanwendung.
8. Öffnen Sie die Konsole und vergewissern Sie sich, dass in den entsprechenden Benutzerkonfigurationen die Host- und Mainframeunterstützung aktiviert ist.
9. Führen Sie den Emulator aus und öffnen Sie die Sitzung.
10. Starten oder aktualisieren Sie Password Manager Agent.

Die Agentsoftware erkennt dann den Verbindungsbildschirm und zeigt ein Formular für die Anmeldeinformationen an, die eingegeben und gespeichert werden müssen.

Password Manager Agent startet nicht

Die Password Manager Agent-Software sollte auf Ihren Clientgeräten, die nicht unter Windows Vista ausgeführt werden, immer als letzte Software installiert werden, die die GINA ändert. Wenn Password Manager Agent zwar installiert ist, jedoch nicht wie erwartet startet, liegt dies möglicherweise an einer unterbrochenen GINA-Kette. Zu einer solchen Unterbrechung kommt es, wenn Software installiert bzw. aktualisiert wird, nachdem Password Manager Agent die Windows-GINA-Kette ändert. Von Softwarepaketen, die die Smartcard-Authentifizierung unterstützen, Novell Clients, Symantec und Presentation Server ist bekannt, dass sie die Windows-GINA-Kette ändern.

Software-Upgrades und die GINA-Kette

Wenn Password Manager bereits installiert ist und Sie beabsichtigen, Software zu installieren bzw. zu aktualisieren, die die Windows-GINA-Kette ändert, empfiehlt Citrix, dass Sie zunächst Password Manager Agent deinstallieren. Nach dem Deinstallieren von Password Manager Agent können Sie die neue Software installieren (bzw. aktualisieren) und dann Password Manager Agent erneut installieren. So wird sichergestellt, dass die richtige DLL-Datei installiert und für die Verwendung mit Password Manager registriert ist.

Empfohlene Schritte zur Neuinstallation

1. Deinstallieren Sie sämtliche Software von Drittanbietern, die die GINA-Kette ändert.
2. Deinstallieren Sie die Agentsoftware.
3. Installieren Sie die Drittanbietersoftware.
4. Installieren Sie die Agentsoftware.

Wenn Sie vor kurzem Drittanbietersoftware aktualisiert oder installiert haben und davon ausgehen, dass diese Software die Windows-GINA-Kette geändert hat, überprüfen Sie den Windows-Registrierungseintrag und das Clientgerät, um festzustellen, ob die DLL-Dateien der GINA-Kette vorhanden sind und sich am korrekten Speicherort befinden. Wenn sich die Dateien nicht auf dem Computer befinden, deinstallieren Sie Password Manager Agent und installieren Sie den Agent anschließend neu.

Wichtig: Beim Deinstallieren von Software, die die GINA-Kette unterbrochen haben könnte, ist es wichtig, die Software auf dem Clientgerät in der umgekehrten Reihenfolge zur Installation zu deinstallieren. Wenn dies nicht beachtet wird, kann es passieren, dass der Computer nicht mehr funktionsfähig ist. Bearbeiten Sie nicht die Registrierung.

Erstellen eines neuen Signaturzertifikates

Der Password Manager-Dienst generiert sowohl unmittelbar vor dem Ablauf des Signaturzertifikates als auch bei dessen Ablauf Ereignisprotokollwarnungen. Erstellen Sie ein neues Zertifikat, um die Ausgabe der Ereignisprotokollwarnungen zu beenden. Verwenden Sie zum Erstellen eines neuen Zertifikates CtxCreateSigningCert.exe. Signieren Sie mit dem Datensignierungstool, CtxSignData.exe, (mit den vom neuen Zertifikat bereitgestellten Schlüsseln) die Daten im zentralen Speicher. Weitere Informationen finden Sie unter „Signieren, Aufheben der Signatur, Neusignieren und Prüfen von Daten“ auf Seite 260.

Ein neues Signaturzertifikat muss nach dem ersten Konfigurieren des Password Manager-Dienstes nur erstellt werden, wenn eine der folgenden Bedingungen eintritt:

- Das Signaturzertifikat läuft demnächst ab oder ist bereits abgelaufen.
- Sie denken, dass die Sicherheit des Signaturzertifikates nicht mehr gegeben ist.

Zum Erstellen eines neuen Zertifikates müssen Sie CtxCreateSigningCert.exe ausführen. Diese Datei befindet sich im Ordner %ProgramFiles%\Citrix\MetaFrame Password Manager\Service. Geben Sie auf dem Computer, auf dem der Password Manager-Dienst ausgeführt wird, an der Eingabeaufforderung **CtxCreateSigningCert.exe** ein.

Geben Sie den Namen der öffentlichen Schlüsseldatei, den Namen der privaten Schlüsseldatei und den Zeitraum (in Monaten) ein, der bis zum Ablauf des Signaturzertifikates vergeht. Damit ist das neue Zertifikat erstellt.

CtxCreateSigningCert

Verwendung:

CtxCreateSigningCert *<Name_öffentliches_Zertifikat>*
<Name_privates_Zertifikat> *<Ablaufzeit_in_Monaten>*

Wobei Folgendes gilt:

<Name_öffentliches_Zertifikat> = Dateiname des öffentlichen Zertifikats

<Name_privates_Zertifikat> = Dateiname des privaten Zertifikats

<Ablaufzeit_in_Monaten> = Anzahl der Monate bis zum Ablauf des Zertifikates

Beispiel:

```
ctxcreatesigningcert “C:\PublicKeyCert.cert”
“C:\PrivateKeyCert.cert” “12”
```

Signieren, Aufheben der Signatur, Neusignieren und Prüfen von Daten

Mit dem Datensignierungstool, CtxSignData.exe, können Sie Daten im zentralen Speicher signieren, die Signatur aufheben, Daten neu signieren und Daten prüfen. Es handelt sich dabei um ein Befehlszeilentool, das auf der Produkt-CD im Ordner \Service zur Verfügung steht. CtxSignData.exe ist ferner unter %ProgramFiles%\Citrix\MetaFrame PasswordManager\Service \SigningTool\CtxSignData.exe auf dem Server installiert, auf dem der Dienst ausgeführt wird.

Hinweis: Das Datensignierungstool wird mit dem Modul **Datenintegrität** des Password Manager-Dienstes installiert. Falls dieses Modul bei der ersten Installation von Password Manager nicht installiert wurde, kann die Installation zu einem späteren Zeitpunkt nachgeholt werden.

Die folgenden Parameter werden mit der Datei CtxSignData.exe verwendet:

- „Signieren von Daten (-s)“ auf Seite 261
- „Neusignieren von Daten (-r)“ auf Seite 262
- „Aufheben der Signatur von Daten (-u)“ auf Seite 264
- „Prüfen von Daten (-v)“ auf Seite 265

So starten Sie das Datensignierungstool

Geben Sie auf dem Computer, auf dem der Password Manager-Dienst ausgeführt wird, an der Eingabeaufforderung **CtxSignData.exe** ein und verwenden Sie die entsprechenden Befehlszeilenparameter (-s, -r, -u, -v).

Signieren von Daten (-s)

Verwenden Sie den Befehlszeilenparameter zum Signieren von Daten (-s), um in Umgebungen mit unsignierten Daten die Datenintegrität zu aktivieren.

Hinweis: Wenn Sie eine Password Manager-Umgebung haben, die ohne Datenintegrität ausgeführt wird, und Sie später beschließen, die Datenintegrität zu implementieren, müssen Sie die Daten im vorhandenen zentralen Speicher mit dem Datensignierungstool signieren.

Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Password Manager-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe, Active Directory oder freigegebener Novell Ordner) angeben. Sämtliche Daten werden gelesen und mit dem neuen Zertifikat signiert.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -s lautet:

```
CtxSignData [-s Dienstpfad Zertifikatdatei
Speicherort_zentraler_Speicher NTFS|NNFS|AD]
```

Wobei Folgendes gilt:

-s	Signieren der Datendateien im zentralen Speicher
Dienstpfad	Pfad zum Password Manager-Dienst im URI-Format
Zertifikatsdatei	Dateiname des Zertifikates, das zum Signieren und Neusignieren von Daten verwendet wird
Speicherort_zentraler_ Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|NNFS|AD	Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • NNFS = Novell Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -s:

```
ctxsigndata -s "mpmserver.meineFirma.com/MPMService"
"C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
```

```
ctxsigndata -s "mpmserver.meineFirma.com/MPMService"
"C:\priv12mos.cert" "\\NVLServer1\SYS\citrixsync" NNFS
```

```
ctxsigndata -s mpmserver.meineFirma.com/MPMService
"C:\priv12mos.cert" DC1.meineFirma.com AD
```

Neusignieren von Daten (-r)

Verwenden Sie den Befehlszeilenparameter für das Neusignieren, wenn das vorhandene Signaturzertifikat demnächst abläuft, bereits abgelaufen ist oder seine Sicherheit nicht mehr gewährleistet ist. Sie müssen den neuen Namen der Signaturzertifikatdatei, den URI für den Password Manager-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe, Active Directory oder freigegebener Novell Ordner) angeben. Sämtliche Daten werden gelesen und geprüft und anschließend mit dem neuen Zertifikat signiert. Änderungen an den Einstellungen in der Konsole bzw. dem Agent sind nicht nötig, da für diese Komponenten die Datenintegrität bereits aktiviert ist.

So signieren Sie zerstörte Daten neu

1. Öffnen Sie die Password Manager Console und gehen Sie zur betroffenen Benutzerkonfiguration.
2. Öffnen Sie die Benutzerkonfiguration, um sicherzustellen, dass die Daten aus dem zentralen Speicher lesbar sind.
3. Schließen Sie die Benutzerkonfiguration, um neue, nicht zerstörte Daten im zentralen Speicher zu speichern.
4. Signieren Sie die Daten im zentralen Speicher mit dem Signierungstool (ctxsigndata) neu.

Hinweis: Falls eine Sicherheitsverletzung zur Zerstörung geführt hat, empfiehlt Citrix, vor dem Neusignieren der Daten das oben beschriebene Verfahren für alle Benutzerkonfigurationen durchzuführen. Auf diese Weise wird verhindert, dass ungesicherte Daten signiert werden.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -r lautet:

```
CtxSignData [-r Dienstpfad Zertifikatdatei
Speicherort_zentraler_Speicher NTFS|NNFS|AD]
```

Wobei Folgendes gilt:

-r	Neusignieren der Datendateien im zentralen Speicher (einschließlich -v)
Dienstpfad	Pfad zum Password Manager-Dienst im URI-Format
Zertifikatsdatei	Dateiname des Zertifikates, das zum Signieren und Neusignieren von Daten verwendet wird
Speicherort_zentraler_ Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|NNFS|AD	Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • NNFS = Novell Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -r:

```
ctxsigndata -r "mpmserver.meineFirma.com/MPMService"
"C:\priv12mos.cert" "\\MPMCentralServer\citrixsync$" NTFS
```

```
ctxsigndata -r "mpmserver.meineFirma.com/MPMService"
"C:\priv12mos.cert" "\\NVLServer1\SYS\citrixsync" NNFS
```

```
ctxsigndata -r "mpmserver.meineFirma.com/MPMService"
"C:\priv3mos.cert" "DC1.meineFirma.com AD
```

Aufheben der Signatur von Daten (-u)

Verwenden Sie den Befehlszeilenparameter für das Aufheben der Signatur von Daten, wenn Sie die Datenintegrität deaktivieren. Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Password Manager-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe, Active Directory oder freigegebener Novell Ordner) angeben. Sämtliche Daten werden ohne Prüfung gelesen und die Signaturen werden entfernt.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -u lautet:

```
CtxSignData [-u Speicherort_zentraler_Speicher NTFS|NNFS|AD]
```

Wobei Folgendes gilt:

-u	Aufheben der Signatur aller Datendateien im zentralen Speicher
Speicherort_zentraler_ Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|NNFS|AD	Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • NNFS = Novell Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -u:

```
ctxsigndata -u "\\MPMCentralServer\citrixsync$" NTFS

ctxsigndata -u "\\NVLServer1\SYS\citrixsync" NNFS

ctxsigndata -u DC1.meineFirma.com AD
```

Prüfen von Daten (-v)

Verwenden Sie den Befehlszeilenparameter für das Prüfen von Daten, um zu überprüfen, ob alle Daten im zentralen Speicher signiert und geprüft sind. Sie müssen den Namen der Signaturzertifikatdatei, den URI für den Password Manager-Dienst, den Speicherort des zentralen Speichers und dessen Typ (NTFS-Netzwerkfreigabe, Active Directory oder freigegebener Novell Ordner) angeben. Sämtliche Daten werden gelesen, geprüft und signiert.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -v lautet:

```
CtxSignData [-v Dienstpfad Speicherort_zentraler_Speicher
NTFS|NNFS|AD]
```

Wobei Folgendes gilt:

-v	Prüfen der Signaturen der Datendateien im zentralen Speicher
Dienstpfad	Pfad zum Password Manager-Dienst im URI-Format
Speicherort_zentraler_ Speicher	UNC-Pfad zum Speicherort der Dateifreigabe bzw. DNS des Active Directory-Domänencontrollers
NTFS|NNFS|AD	Typ des zentralen Speichers für den Verzeichnisdienst, wobei: • NTFS = Microsoft NTFS-Dateifreigabe • NNFS = Novell Dateifreigabe • AD = Microsoft Active Directory

Im Anschluss finden Sie Beispiele des CtxSignData-Befehls mit dem Parameter -v:

```
ctxsigndata -v "mpmserver.meineFirma.com/MPMService"
"\\MPMCentralServer\citrixsync$" NTFS
```

```
ctxsigndata -v "mpmserver.meineFirma.com/MPMService"
"\\NVLServer1\SYS\citrixsync" NNFS
```

```
ctxsigndata -v "mpmserver.meineFirma.com/MPMService"
"https://mpmserver.meineFirma.com/MPMService" DC1.meineFirma.com AD
```

Anzeigen der Hilfe (-h)

Verwenden Sie den Befehlszeichenparameter -h, um die Hilfe für den CtxSignData-Befehl anzuzeigen.

Die Syntax für den CtxSignData-Befehl mit dem Parameter -h lautet:

```
CtxSignData [-h]
```

Wobei Folgendes gilt:

-h	Anzeigen der Hilfe

Im Anschluss finden Sie ein Beispiel des CtxSignData-Befehls mit dem Parameter -h:

```
ctxsigndata -h
```

Aktivieren und Deaktivieren des Datenintegritätsdienstes in der Password Manager Agent-Software

Die Datenintegrität für die Password Manager Agent-Software kann durch Bearbeiten des folgenden Registrierungsschlüssels aktiviert bzw. deaktiviert werden:

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extensions\SyncManager\PerformIntegrityCheck

Typ: DWORD

Werte:

0 = Prüfung der Datenintegrität deaktiviert

1 = Prüfung der Datenintegrität aktiviert

Entfernen gelöschter Objekte im zentralen Speicher

CtxFileSyncClean.exe entfernt alle Objekte im zentralen Speicher, die auf gelöschte Objekte verweisen. So wird sichergestellt, dass die Umgebung wirklich nur die aktuellen Informationen enthält. Führen Sie zum Entfernen CtxFileSyncClean.exe aus. Diese Datei finden Sie im Verzeichnis \Tools auf der Produkt-CD.

Verschieben von Daten in einen anderen zentralen Speicher

Hinweis: Beim Import administrativer Daten in die Password Manager Consolewerden nur neue, vom Administrator erstellte Kennwortrichtlinien überschrieben. Die Standard- und Domänenrichtlinien werden nicht importiert und daher bleiben Änderungen erhalten.

Es kann aus verschiedenen Gründen sinnvoll sein, Kennwortrichtlinien, Anwendungsvorlagen, Anwendungsdefinitionen, Sicherheitsfragen und andere Typen von administrativen Daten in Password Manager zu migrieren. Diese Gründe sind wie folgt:

- Der Benutzer verwendet eine neue Domäne.
- Der Password Manager-Umgebung wird ein neuer Server hinzugefügt.
- Eine neue Domäne wird hinzugefügt, sodass Benutzer die Kontozuordnungsfunktion von Password Manager verwenden können.
- Die Benutzer verwenden die Kontozuordnung domänenübergreifend.
- Password Manager wird von einer Testumgebung in eine Produktionsumgebung verschoben.

Die Schritte für das Migrieren von administrativen Daten sind immer gleich, egal, welche Gründe es für die Migration gibt. In allen Fällen müssen Sie die administrativen Daten zuerst aus der bestehenden Umgebung exportieren und dann in die neue Umgebung importieren. Meistens müssen Sie auch die Benutzer auf den neuen zentralen Speicher umleiten. Die genannten Aufgaben werden mit den Befehlen in der Password Manager Console ausgeführt.

Der folgenden Tabelle können Sie entnehmen, welche Daten mit dem Befehl **Exportieren** migriert werden können:

Migrierbar	Nicht migrierbar
Kennwortrichtlinien (außer für die Standard- und Domänenrichtlinie)	Benutzerkonfigurationen
Anwendungsvorlagen	People-Ordner
Anwendungsdefinitionen	Anwendungsgruppen
Sicherheitsfragen und Sicherheitsfragengruppen, die für die fragenbasierte Authentifizierung verwendet werden	Benutzerinformationen für die Anmeldung
	Fragenkataloge

Benutzerkonfigurationen werden nicht automatisch von einem zentralen Speicher auf einen anderen zentralen Speicher migriert. Sie müssen die Benutzerkonfigurationen stattdessen neu erstellen und die Benutzer auf den neuen zentralen Speicher umleiten. Wenn Password Manager Agent die Daten mit den Daten im zentralen Originalspeicher synchronisiert, erkennt die Software geänderte Werte. Password Manager Agent kopiert dann die Anmeldeinformationen in den neuen zentralen Speicher.

Wichtig: Verweisen Sie den Password Manager-Dienst mit dem Dienstkonfigurationstool auf den neuen zentralen Speicher.

Migrieren von Daten auf einen neuen zentralen Speicher

Exportieren Sie die administrativen Daten mit der Password Manager Console. Beim Exportieren der Daten aus dem ursprünglichen zentralen Speicher erstellt Password Manager eine XML-Datei mit den administrativen Daten. Die Informationen in dieser Datei müssen Sie dann in den neuen zentralen Speicher importieren.

So exportieren Sie administrative Daten

1. Klicken Sie in der ursprünglichen Konsole auf den Password Manager-Knoten und anschließend auf **Administrative Daten exportieren**.

   Der Assistent für das Exportieren administrativer Daten wird angezeigt.

2. Klicken Sie auf der Seite **Willkommen** auf **Weiter**.
3. Wählen Sie auf der Seite **Daten auswählen** die Datentypen aus, die Sie exportieren möchten, und klicken Sie auf **Weiter**.
4. Speichern Sie die Daten auf der Seite **Datei angeben** in einer XML-Datei an einem Speicherort, auf den Sie vom Computer der neuen Konsole aus zugreifen können, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Daten exportieren** auf **Fertig stellen**.

   Der Assistent für das Exportieren administrativer Daten wird geschlossen.

So importieren Sie administrative Daten

1. Installieren Sie Password Manager am neuen Speicherort und starten Sie die Agentsoftware mit dem Task **Discovery konfigurieren und durchführen**.
2. Klicken Sie in der ursprünglichen Konsole auf den Password Manager-Knoten und anschließend auf **Administrative Daten importieren**.

   Der Assistent für das Importieren administrativer Daten wird angezeigt.

3. Klicken Sie im Begrüßungsbildschirm auf **Next**.

4. Wählen Sie auf der Seite **Datei angeben** die exportierte XML-Datendatei aus und klicken Sie auf **Weiter**.

   Sie werden darauf hingewiesen, wenn die Inhalte der Datendatei und der zentrale Zielspeicher Namen oder IDs gemeinsam verwenden. In diesen Situationen können Sie mit den Schaltflächen **Ja**, **Ja zu allen** und **Nein** die bestehenden Inhalte im zentralen Speicher überschreiben oder beibehalten.

5. Klicken Sie auf der Seite **Daten importieren** auf **Fertig stellen**.

   Der Assistent für das Importieren administrativer Daten wird geschlossen.

Umleiten von Benutzern auf den neuen zentralen Speicher

1. Erstellen Sie nach der Migration der Daten auf den neuen zentralen Speicher neue Benutzerkonfigurationen in der neuen Konsole.

   Wichtig: Falls der Password Manager-Dienst auch auf den neuen Computer migriert wird, müssen Sie die neue Dienstadresse in die Benutzerkonfigurationen einfügen.

   ---

2. Wählen Sie die Benutzerkonfiguration, die auf den neuen zentralen Speicher umgeleitet werden soll, in der ursprünglichen Konsole aus und klicken Sie auf **Benutzer umleiten**.

3. Geben Sie im Dialogfeld **Benutzer umleiten** den Typ und den Speicherort des neuen zentralen Speichers an und klicken Sie auf **OK**.

   Das Dialogfeld wird geschlossen und die Benutzerkonfiguration verweist jetzt auf den neuen zentralen Speicher.

Hinweis: Der Befehl zum Umleiten von Benutzern deaktiviert die Einstellung **Datenordner und Registrierungsschlüssel des Benutzers beim Beenden des Agents löschen**. So wird sichergestellt, dass Agents alle im lokalen Speicher der Benutzer vorhandenen Daten beibehalten, einschließlich der Anmeldeinformationen, Einstellungen und Informationen zum Umleiten der Benutzer auf den neuen zentralen Speicher. Diese Einstellung muss in der neuen Umgebung so lange deaktiviert bleiben, bis die Registrierung auf dem Password Manager Agent-Gerät geändert wird und auf den Speicherort des neuen zentralen Speichers verweist.

In einigen Umgebungen werden die Benutzerprofile beim Abmelden automatisch gelöscht. Wenn dies der Fall ist, können Sie entweder das Löschen der Benutzerprofile deaktivieren, sodass Agents auf den neuen zentralen Speicher umgeleitet werden, oder Sie können eine Umleitung durchführen und die Benutzer veranlassen, Password Manager Agent zu aktualisieren, um die Synchronisierung zu erzwingen. Bei der erzwungenen Synchronisierung werden die Benutzeranmeldeinformationen in den neuen zentralen Speicher kopiert.

Hinweis: Während einer Umleitung müssen alle Benutzer, die umgeleitet werden, angemeldet sein. Password Manager Agent wird aktualisiert, sobald die Anmeldeinformationen von Password Manager Agent bereitgestellt wurden.

Sichern von wichtigen Dateien

Stellen Sie sicher, dass Backupmaßnahmen im Unternehmen auch regelmäßig Sicherungskopien des zentralen Speichers mit dem Inhalt, den Zertifikaten und den persönlichen und privaten Schlüsseln angefertigt werden.

Wichtig: Wenn Sie als zentralen Speicher eine NTFS-Netzwerkfreigabe oder einen freigegebenen Novell Ordner verwenden, müssen Sie die Berechtigungen für diese Dateien in Windows ändern, sodass das Backupprogramm darauf zugreifen kann.

Sichern von Dateien des Password Manager-Dienstes

In den folgenden Schritten wird beschrieben, wie Sie den Citrix Password Manager-Dienst sichern und wiederherstellen.

Hinweis: Weitere Informationen finden Sie unter „Verwenden des Tools CtxMoveKeyRecoveryData Tool zum Sichern von Dienstdaten“ im *Citrix Password Manager-Installationshandbuch*.

So sichern Sie den Dienst ab

1. Notieren Sie sich die Einstellungen, die Sie vornehmen, wenn Sie das Dienstkonfigurationstool zum Einrichten des Dienstes ausführen.
2. Exportieren Sie den Dienst unter Verwendung von CtxMoveServiceData.exe auf eine sichere Dateifreigabe bzw. ein sicheres Speichermedium:
   A. Öffnen Sie eine Eingabeaufforderung und gehen Sie zu C:\Programme\Citrix\Metaframe Password Manager\Service\Tools.

   B. Geben Sie Folgendes ein:
   CtxMoveServiceData.exe –export\\server\share\backupfile

   Hinweis: Verwenden Sie bei der Pfadangabe keine Umgebungsvariablen.

   C. Geben Sie ein beliebiges Kennwort ein, wenn Sie dazu aufgefordert werden. Notieren Sie sich das Kennwort.

   Wichtig: Die Dienstdaten, die Sie in der Sicherungskopie speichern, werden mit diesem Kennwort verschlüsselt. Bewahren Sie das Kennwort an einem sicheren Ort auf.

   D. Geben Sie das Kennwort erneut ein, wenn Sie dazu aufgefordert werden.

   E. Überprüfen Sie, ob die Sicherungskopie erstellt wurde.

So stellen Sie den Dienst wieder her

1. Installieren Sie den Dienst von den Installationsmedien.
2. Konfigurieren Sie den Dienst mit den richtigen Einstellungen. Nutzen Sie dafür die Notizen, die Sie sich vor der Sicherung gemacht haben.

   Hinweis: Wenn Sie die Datenintegrität implementiert haben, müssen Sie den Serverstandort für die Datenintegrität korrekt konfigurieren, d. h. Sie müssen angeben, ob sich der Serverstandort für die Datenintegrität geändert hat oder gleich geblieben ist.

   ---

3. Schließen Sie die Konfiguration ab und starten Sie den Dienst neu. Falls erwünscht, kann der Dienst sofort nach dem Starten wieder beendet werden.
4. Importieren Sie den Dienst unter Verwendung von CtxMoveServiceData.exe von einer sicheren Dateifreigabe bzw. einem sicheren Speichermedium:
   A. Öffnen Sie eine Eingabeaufforderung und gehen Sie zu C:\Programme\Citrix\Metaframe Password Manager\Service\Tools.
   B. Geben Sie Folgendes ein: **CtxMoveServiceData.exe –import <\\Server\Freigabe\Backup-datei>**
   C. Wenn Sie dazu aufgefordert werden, geben Sie das korrekte Kennwort ein.
   D. Wenn Sie gefragt werden, ob Sie AKR.DAT überschreiben möchten, wählen Sie **Ja**.
5. Starten Sie den Dienst. Der Dienst kann nun verwendet werden.

11

Liste der Password Manager-Einstellungen

Einstellungsreferenz für Password Manager 4.6

In dieser Referenz werden die Einstellungen und die Standwerte beschrieben, die im Knoten **Password Manager** der Access Management Console zur Verfügung stehen. Die Einträge sind in der Reihenfolge der Position der Konsole aufgeführt.

Zum Nachschlagen einer bestimmten Einstellung können Sie unter „Liste der Password Manager-Einstellungen“ auf den Namen der Einstellung klicken. Über diesen Hyperlink gelangen Sie direkt zur Definition der Einstellung (mit Angabe der Standardeinstellung).

Benutzerkonfigurationen

In diesem Abschnitt werden die Einstellungen und Steuerelemente von Benutzerkonfigurationen beschrieben. Alle Hinweise zur Navigation in diesem Abschnitt beziehen sich auf das Bearbeiten einer vorhandenen Benutzerkonfiguration. Zum Dialogfeld **Benutzerkonfiguration bearbeiten** gelangen Sie folgendermaßen:

Managementkonsolen > Access Management Console > Password Manager > Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten

Synchronisierungsserver

Diese Einstellung gibt den Domänencontroller an, der Benutzer bei der Synchronisierung mit dem zentralen Speicher bindet.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Synchronisierungsserver

Grundlegendes Agentverhalten

Mit diesen Steuerelementen wird das Agentverhalten für diese Benutzer-konfiguration angepasst. Die Einstellungen für die Agentbenutzeroberfläche und die Synchronisierung werden hier festgelegt.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Grundlegendes Agentverhalten

Benutzerseitiges Anzeigen aller Kennwörter im Anmeldungsmanager

Diese Einstellung steuert, ob die Benutzer im Anmeldungsmanager Kennwörter anzeigen dürfen. Wenn die Einstellung nicht aktiviert ist, ist die Schaltfläche **Anzeigen** im Anmeldungsmanager deaktiviert. Wenn Sie die Kennwortanzeige auf bestimmte Anwendungen beschränken möchten, aktivieren Sie diese Einstellung und steuern Sie dann mit der entsprechenden Einstellung für die Kennwortrichtlinie, ob Benutzer die Kennwörter für Anwendungen anzeigen können, die von dieser Richtlinie verwaltet werden.

Standardeinstellung: Nicht ausgewählt

Neuauthentifizierung vor dem Anzeigen der Benutzerkennwörter erzwingen

Diese Einstellung steuert, ob sich Benutzer erneut an Citrix Password Manager authentifizieren müssen, bevor die Kennwörter angezeigt werden.

Standardeinstellung: Ausgewählt

Benutzerseitiges Anhalten des Agents

Diese Einstellung steuert, ob die Benutzer Citrix Password Manager Agent vorübergehend anhalten können. Wenn sie aktiviert ist, können die Benutzer den Agent anhalten, ohne die Anwendung zu beenden. Wenn der Agent angehalten ist, erkennt Citrix Password Manager keine Anwendungen, für die eine Authentifizierung erforderlich ist und die Benutzer müssen die eigenen Anmeldeinformationen eingeben und senden.

Standardeinstellung: Ausgewählt

Benutzer über Fehlschlagen der Agentsynchronisierung benachrichtigen

Aktivieren Sie diese Einstellung, wenn die Benutzer benachrichtigt werden sollen, wenn die Agentsynchronisierung fehlschlägt.

Standardeinstellung: Ausgewählt

Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern

Diese Einstellung steuert, ob der Agent den Benutzer auffordert, Anmeldeinformationen für neue Anwendungen hinzuzufügen. Deaktivieren Sie diese Einstellung, um Benutzer zu zwingen, alle Anmeldeinformationen manuell im Anmeldungsmanager einzugeben. Wenn diese Einstellung nicht aktiviert ist, hat die Einstellung **Benutzer können das Speichern der Anmeldeinfo bei Erkennung einer neuen Anwendung abbrechen** in den clientseitigen Interaktionseinstellungen keine Wirkung.

Standardeinstellung: Ausgewählt

Definierte Formulare automatisch verarbeiten, wenn sie von der Agentsoftware erkannt werden

Aktivieren Sie diese Option, damit die Agentsoftware gespeicherte Anmeldeinformationen automatisch ohne Eingriff des Benutzers senden darf. Wenn Sie die dazugehörige Einstellung **Agent sendet dieses Formular automatisch** in der dieser Benutzerkonfiguration zugeordneten Anwendungsdefinition aktiviert haben, werden die Felder zur Eingabe der Anmeldeinformationen in der Anwendung automatisch ausgefüllt.

Standardeinstellung: Ausgewählt

Zeitraum zwischen Agent-Anfragen für die Neuauthentifizierung

In dieser Einstellung wird der Zeitraum zwischen Agentanfragen zur Neuauthentifizierung festgelegt. Wenn der angegebene Zeitraum abläuft, wird die Arbeitsstation gesperrt und Benutzer müssen die primären Anmeldeinformationen eingeben, um sich neu zu authentifizieren. Mit dieser Methode kann geprüft werden, ob der Benutzer, der die Sitzung initiiert hat, weiterhin an der Arbeitsstation arbeitet. Der Mindestwert für diese Einstellung ist 1 Minute.

Standardeinstellung: 8 Stunden

Agentbenutzeroberfläche

Mit diesen Einstellungen wird der Inhalt des QuickInfo des Symbols eingestellt, das Citrix Password Manager-Symbol angezeigt oder ausgeblendet und die Verzögerung für das Senden der Anmeldeinformationen festgelegt.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Agentbenutzeroberfläche

Computername in QuickInfo des Infobereichssymbols anzeigen

Aktivieren Sie diese Einstellung, wenn der Computername im QuickInfo des Infobereichssymbols angezeigt werden soll.

Standardeinstellung: Nicht ausgewählt

Symbol im Infobereich anzeigen

Aktivieren Sie dieses Steuerelement, wenn das Citrix Password Manager-Symbol im Infobereich angezeigt werden soll, wenn der Agent aktiv ist. Wenn das Symbol nicht aktiviert ist, können die Benutzer die Agentsoftware nicht starten oder beenden oder auf andere benutzergesteuerte Optionen zugreifen.

Standardeinstellung: Ausgewählt

Verzögerung für das agentseitige Senden der Anmeldeinformationen angeben

Aktivieren Sie diese Einstellung, um anzugeben, wie lange der Agent nach dem Erkennen einer zulässigen Anwendung das Senden der Anmeldeinformationen verzögert. Wenn diese Einstellung aktiviert ist, können Sie angeben, um wie viele Sekunden das Senden der Anmeldeinformationen verzögert werden soll. Stellen Sie mit dieser Einstellung sicher, dass die Anwendung zum Empfang der Anmeldeinformationen bereit ist. Wenn die Einstellung aktiviert ist, zeigt die Agentsoftware während der Verzögerung ein animiertes Symbol an, das angibt, dass der Agent einen Vorgang ausführt.

Standardeinstellung: Nicht ausgewählt

Im Anmeldungsmanager standardmäßig angezeigte Spalten und -reihenfolge festlegen

Diese Einstellung steuert, welche Spalten und in welcher Reihenfolge die Spalten in der Detailansicht des Anmeldungsmanagers angezeigt werden. Diese Einstellung hat keine Auswirkung auf die Ansichten **Liste** oder **Symbol** im Anmeldungsmanager.

Standardeinstellung:

Anwendungsname

Beschreibung

Gruppe

Letzte Verwendung

Geändert

Kennwort

URL/Modul

Benutzername/ID

Clientseitiges Verhalten

Mit diesen Einstellungen werden die Kennwortzuordnung, die Agent-Ereignis-protokollierung, die Speicherung der Registrierungsschlüssel beim Beenden und die Speicherung von Anmeldeinformationen bei neu erkannten Anwendungen konfiguriert.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Clientseitiges Verhalten

Kennwortzuordnung bei der Ersteinrichtung der Anmeldeinformationen erzwingen

Aktivieren Sie dieses Steuerelement, wenn die Benutzer bei der Ersteinrichtung der Anmeldeinformationen das Kennwort zur Bestätigung zweimal eingeben sollen.

Standardeinstellung: Ausgewählt

Citrix Password Manager-Ereignisse mit der Windows-Ereignisprotokollierung aufzeichnen

Aktivieren Sie dieses Steuerelement, um Fehler- und Warnereignisse des Agents mit der Windows-Ereignisprotokollierung aufzuzeichnen.

Standardeinstellung: Nicht ausgewählt

Datenordner und Registrierungsschlüssel des Benutzers beim Beenden der Agentsoftware löschen

Aktivieren Sie dieses Steuerelement, wenn die Registrierungsschlüssel und Datenordner des Benutzers, einschließlich der verschlüsselten Anmeldeinformationen, beim Beenden der Agentsoftware gelöscht werden sollen.

Standardeinstellung: Nicht ausgewählt

Benutzer können das Speichern der Anmeldeinfo bei Erkennung einer neuen Anwendung abbrechen

Mit dieser Einstellung steuern Sie, ob Benutzer zum Speichern der Anmeldeinformationen aufgefordert werden, wenn der Agent eine Anwendung erkennt, für die keine Anmeldeinformationen gespeichert sind. Wenn die Option aktiviert ist, können die Benutzer wählen, ob sie die Anmeldeinformationen im Anmeldungsmanager jetzt, später oder nie speichern möchten. Wenn die Einstellung **Anwendungen automatisch erkennen und Benutzer zum Speichern der Anmeldeinformationen auffordern** nicht aktiviert ist, fordert die Agentsoftware die Benutzer nicht zum Speichern der Anmeldeinformationen auf.

Standardeinstellung: Ausgewählt

Anzahl der Tage einschränken, für die gelöschte Anmeldeinformationen verfolgt werden

Mit diesen Steuerelementen können Sie angeben, wie lange der zentrale Speicher Anmeldeinformationen verfolgt, die vom Anmeldungsmanager gelöscht wurden. Wenn Anmeldeinformationen des Benutzers auf mehreren Clientgeräten gespeichert werden, löscht der Agent die Anmeldeinformationen, wenn in diesem Zeitraum eine Synchronisierung mit dem zentralen Speicher erfolgt. Wenn die Anmeldeinformationen beim Ablauf des Zeitraums immer noch auf dem Clientgerät gespeichert sind, werden sie wiederhergestellt, wenn der Agent mit dem zentralen Speicher synchronisiert wird.

Standardeinstellung: Ausgewählt/180 Tage

Synchronisierung

Mit diesen Steuerelementen werden die folgenden Optionen eingestellt: benutzerseitiges Aktualisieren der Agenteinstellungen, Synchronisieren der Konfigurationsinformationen des Benutzers, Ausführen der Agentsoftware, wenn die Verbindung mit dem zentralen Speicher nicht mehr möglich ist sowie der Zeitraum zwischen automatischen Synchronisierungsanfragen.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Synchronisierung

Benutzer können Agenteinstellungen aktualisieren

Aktivieren Sie diese Einstellung, um den Benutzern das Aktualisieren der Agent-einstellungen im Anmeldungsmanager zu erlauben. Wenn die Einstellung nicht aktiviert ist, ist die Schaltfläche **Anzeigen** im Anmeldungsmanager deaktiviert.

Standardeinstellung: Ausgewählt

Beim Start erkannter Anwendungen/des Anmeldungsmanagers synchronisieren

Aktivieren Sie diese Einstellung, wenn der Agent die Benutzerkonfigurations-informationen immer dann synchronisieren soll, wenn ein Benutzer eine erkannte Anwendung oder den Anmeldungsmanager startet. Häufiges Synchronisieren kann die Leistung auf dem Client und Server beeinträchtigen und den Netzwerkdatenverkehr erhöhen.

Standardeinstellung: Nicht ausgewählt

Agentausführung ohne Wiederverbindung zum zentralen Speicher zulassen

Diese Einstellung steuert, ob Citrix Password Manager ausgeführt wird, wenn für die Synchronisierung keine Verbindung zum zentralen Speicher hergestellt werden kann. Bei Aktivierung dieser Option wird eine lizenzierte Agentinstanz weiter ausgeführt, selbst wenn die Verbindung fehlschlägt. Bei Deaktivierung der Einstellung wird der Agent nur ausgeführt, wenn eine Verbindung zum zentralen Speicher besteht.

Standardeinstellung: Ausgewählt

Zeitraum zwischen automatischen Synchronisierungsanfragen

Mit diesen Steuerelementen wird der Zeitraum zwischen automatischen Synchronisierungsanfragen angegeben. Die automatische Synchronisierung hängt nicht von der Benutzeraktivität ab und wird zusätzlich zu anderen Ereignissen ausgeführt, die eine Synchronisierung auslösen.

Standardeinstellung: Nicht ausgewählt/0 Minuten

Zugriff auf Anmeldeinfo über das Modul „Synchronisierung der Anmeldeinformationen“ zulassen

Aktivieren Sie diese Einstellung, um Remoteclients zu erlauben, über den Dienst auf die Anmeldeinformationen der Benutzer zuzugreifen. Diese Einstellung steuert, ob Remoteclients über das Dienstmodul auf die Anmeldeinformationen der Benutzer zugreifen können. Diese Option wird zusammen mit der Konto-zuordnung verwendet. Mit dieser Funktion kann sich ein Agentbenutzer mit einem oder mehreren Windows-Konten an jeder Anwendung anmelden.

Standardeinstellung: Nicht ausgewählt

Kontozuordnung

Da Unternehmen über mehrere Windows-Domänen verfügen können, können Benutzer auch mehrere Windows-Konten haben. Mit den Optionen zur Kontozuordnung kann sich ein Agentbenutzer mit jedem Windows-Konto des Benutzers an jeder Anwendung anmelden. Mit dieser Steuerelementen können die Benutzer die Anmeldeinformationen mehrerer Windows-Konten zuordnen

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Kontozuordnung

Benutzer können Konten zuordnen

Aktivieren Sie diese Einstellung, um den Benutzern zu erlauben, mehrere Windows-Konten zuzuordnen und die URL sowie den Port anzugeben, an dem das Modul **Synchronisierung der Anmeldeinformationen** installiert ist. Bei der Erstkonfiguration einer Benutzerkonfiguration kann diese Option nicht eingestellt werden. Sie kann nur beim Bearbeiten einer vorhandenen Konfiguration definiert werden.

Standardeinstellung: Nicht ausgewählt

Standarddienstadresse angeben

Aktivieren Sie diese Einstellung, wenn die Standarddienstadresse und der Dienstport des Moduls **Synchronisierung der Anmeldeinformationen** definiert werden sollen. Nach der Definition der Einstellungen können Sie die Option **Wird überprüft** auswählen, um den Adresspfad und den Dienstport zu überprüfen.

Standardeinstellung: <AdresseDesServers > /MPMService/

Dienstport: 443

Benutzer können Dienstadresse bearbeiten

Wenn eine Dienstadresse definiert wurde, können Sie durch Aktivierung dieser Einstellung festlegen, dass die Benutzer die Einstellungen über die Agentbenutzeroberfläche bearbeiten können. Aktivieren Sie diese Option, wenn die Anmeldeinformationen an mehreren Stellen synchronisiert werden, und die Benutzer die Möglichkeit zum Wechseln haben müssen.

Standardeinstellung: Nicht ausgewählt

Standarddomäne angeben

Aktivieren Sie diese Einstellung, um die Standarddomäne anzugeben, die für die Authentifizierung verwendet wird, wenn der Agent mit dem zugeordneten Windows-Konto synchronisiert wird. Wenn diese Einstellung aktiviert ist, können Sie den Standarddomänennamen im entsprechenden Feld eingeben. Wenn Sie die Domäne nicht angeben, wissen die Benutzer möglicherweise nicht, welche Anmeldeinformationen eingegeben werden sollen.

Standardeinstellung: Nicht ausgewählt

Benutzer können Domäne bearbeiten

Aktivieren Sie diese Einstellung, um den Benutzern zu erlauben, die Standarddomäne zu bearbeiten, die für die Authentifizierung verwendet wird, wenn der Agent mit dem zugeordneten Windows-Konto synchronisiert wird.

Standardeinstellung: Nicht ausgewählt

Benutzer können Kennwort speichern

Aktivieren Sie diese Einstellung, um den Benutzern zu erlauben, das Kennwort ihres zugewiesenen Windows-Kontos im Agent zu speichern.

Standardeinstellung: Nicht ausgewählt

Anwendungsunterstützung

Mit diesen Steuerelementen werden die folgenden Optionen eingestellt: Erkennen bestimmter clientseitiger Anwendungsdefinitionen von der Agentsoftware, Aktivieren der Unterstützung für den Terminalemulator und Definieren der Mindestanzahl der Domänennamenstufen für die Zuordnung für Webanwendungen.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Anwendungsunterstützung

Clientseitige Anwendungsdefinitionen erkennen

Aktivieren Sie diese Einstellung, um festzulegen, dass Password Manager von Administratoren festgelegte sowie bestimmte weitere Anwendungen erkennen kann. Diese Einstellung ist standardmäßig aktiviert.

Wenn diese Einstellung aktiviert ist, muss eine der folgenden Optionen ausgewählt werden:

- **Alle Anwendungen**

  Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator oder einem Benutzer (im Anmeldungsmanager) und bei der Installation in den Standardeinstellungen definiert wurden.

- **Nur Anwendungen, die in Password Manager Agent eingeschlossen sind**

  Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator und in den Standardeinstellungen bei der Installation definiert sind. Die Benutzer können keine eigenen Anwendungsdefinitionen im Anmeldungsmanager erstellen.

- **Nur Anwendungen, die von Benutzern im Anmeldungsmanager definiert sind**

  Die Agentsoftware erkennt und reagiert auf Anwendungen, die von einem Administrator und einem Benutzer im Anmeldungsmanager festgelegt sind. Die Agentsoftware erkennt und beantwortet keine Anfragen von Anwendungen, die bei der Installation in den Standardeinstellungen definiert wurden.

Standardeinstellung: Alle Anwendungen

Support für Terminalemulatoren aktivieren

Diese Einstellung steuert die Unterstützung von Terminalemulationsprogrammen. Für die Agentsoftware ist die Unterstützung von Terminalemulatoren erforderlich, um Host- oder Mainframeanwendungen zu erkennen. Bei Aktivierung der Option führt die Agentsoftware einen Prozess aus, der Terminalemulatoren erkennt.

Standardeinstellung: Nicht ausgewählt

Zeitintervall, in dem der Agent auf Terminalemulatorenänderungen prüft

Mit dieser Einstellung wird angegeben, nach welchem Zeitraum die Agentsoftware prüft, ob beim Hostemulator Bildschirmänderungen aufgetreten sind. Niedrigere Werte können mehr CPU-Zeit auf dem Client belegen und den Netzwerkdatenverkehr erhöhen. Wenn die Option nicht aktiviert ist, verwendet die Agentsoftware in der Standardeinstellung 3000 Millisekunden. Wenn die Option aktiviert ist, geben Sie die Zeit in Millisekunden an.

Standardeinstellung: Nicht ausgewählt

Anzahl der Domänennamenstufen für Zuordnung

Mit dieser Einstellung wird die Mindestanzahl der Domänennamenstufen für die Zuordnung für zulässige Webanwendungen angegeben. Bei einem Wert von 2 oder kleiner wird *.domäne1.obersteDomäne zugeordnet; bei einem Wert von 3 wird *.domäne2.domäne1.obersteDomäne zugeordnet. Domänennamenstufen, die über dem angegebenen Wert liegen, werden als Platzhalter behandelt. Wenn Sie die URL-Zuordnung für Webanwendungen stark steuern möchten, legen Sie die strikte URL-Zuordnung in den Anwendungsdefinitionen fest.

Standardeinstellung: 99

Hotdesktop

Diese Steuerelemente legen Folgendes fest:

- Den Pfad der Datei mit den Sitzungseinstellungen, in der die Skripte definiert sind, die am Anfang und Ende einer Hotdesktop-Sitzung ausgeführt werden.
- Den Zeitraum (in Minuten), für den eine Hotdesktop-Sitzung aktiv ist, wenn die Arbeitsstation im Leerlauf ist.
- Den Zeitraum, für den eine Hotdesktop-Sitzung ausgeführt wird, wenn der Desktop gesperrt ist.
- Ob ein Fenster aktiviert ist, das die Hotdesktop-Sitzung kennzeichnet.
- Die in der Hotdesktop-Sitzungsanzeige angezeigte Grafik.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Hotdesktop

Skriptpfad für Sitzungseinstellungen

Dieses Steuerelement gibt den Pfad der Datei mit den Sitzungseinstellungen an, in der die Skripts definiert sind, die am Anfang und Ende einer Hotdesktop-Sitzung ausgeführt werden. Sie können mit dem Skript am Sitzungsanfang auch Anwendungen starten. Mit dem Skript zum Beenden können Aufräumarbeiten, wie z. B. das Entfernen von Dateien, ausgeführt werden. Alle Benutzer müssen auf die Datei zugreifen können.

Standardeinstellung: [keine Eingabe]

Sperrtimeout

Mit diesem Steuerelement wird angegeben, wie viele Minuten eine Hotdesktop-Sitzung aktiv ist, wenn die Arbeitsstation im Leerlauf ist. Nach dem Ablauf des Intervalls wird der Desktop gesperrt.

Standardeinstellung: Alle 10 Minuten

Sitzungstimeout

Mit diesem Steuerelement wird angegeben, wie viele Minuten eine Hotdesktop-Sitzung ausgeführt wird, wenn der Desktop gesperrt ist. Nach Ablauf des Zeitraums wird die Sitzung beendet, und eine neue Sitzung wird gestartet, wenn die Sperrung des Desktops aufgehoben wird.

Standardeinstellung: Alle 5 Minuten

Sitzungsanzeige aktivieren

Diese Einstellung steuert, ob ein Fenster aktiviert ist, das die Hotdesktop-Sitzung kennzeichnet. Bei Aktivierung der Option wird in Hotdesktop-Sitzungen ein transparentes, verschiebbares Fenster auf dem Desktop angezeigt. Das Fenster zeigt den Namen des Benutzers und die Dauer der aktiven Sitzung an.

Standardeinstellung: Ausgewählt

Grafik aktivieren

Mit diesem Steuerelement wird der Pfad der Grafikdatei angegeben, die in der Anzeige der Hotdesktop-Sitzung angezeigt wird. Die angegebene Datei muss im Windows-Bitmap-Dateiformat (.bmp) in einem Verzeichnis gespeichert sein, auf das alle Benutzer zugreifen können.

Standardeinstellung: [Keine]

Lizenzierung

Mit diesen Steuerelementen werden der Name des Lizenzservers und der Zugangsport angegeben, das Lizenzierungsmodell ausgewählt und die Konfiguration ohne Prüfung der Lizenzinformationen fortgesetzt.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Lizenzierung

Name des Lizenzservers

Hier werden der vollqualifizierte Name (*Hostname.Domäne.tld*) und der Zugangsport des Lizenzservers angegeben. Der Standardport ist 27000.

Standardeinstellung: [keine Eingabe]

Standardport: 27000

Standard verwenden (für Portnummer des Lizenzservers)

Aktivieren Sie diese Einstellung, um den Standardwert für den Zugangsport auf dem Lizenzserver zu verwenden. Wenn der Lizenzserver einen anderen Port als den Standardport abhört, deaktivieren Sie diese Einstellung und geben Sie den Zugangsport im entsprechenden Feld ein.

Standardeinstellung: Ausgewählt

Standardport: 27000

Benannte Benutzerlizenzierung (nur Enterprise und Advanced Editionen)

Diese Option ist aktiviert, wenn Sie als Produktedition Password Manager Advanced ausgewählt haben. Sie können diese Option auch auswählen, wenn Sie als Produktedition Password Manager Enterprise einstellen. Mit diesem Lizenztyp kann Password Manager nur von bestimmten, benannten Benutzern verwendet werden. Wenn diese Option aktiviert ist, müssen Sie angeben, wie lange (in Tagen, Stunden und Minuten) die Lizenz dem benannten Benutzer zugeordnet ist, bevor die Lizenz abläuft und der Agent eine neue Verbindung zum Lizenzserver herstellt. Während des angegebenen Zeitraums wird die Lizenzverwaltung vom Benutzer gesteuert, auch wenn sein PC heruntergefahren wird.

Standardeinstellung: Aktiviert *bei der Password Manager Advanced Edition*; nicht verfügbar mit der *Presentation Server Platinum Edition*

Standardeinstellung für die Verbindungstrennung: 21 Tage

CCU-Lizenzierung (nur Enterprise und Platinium Edition)

Diese Option ist automatisch aktiviert, wenn Sie als Produktedition Password Manager Enterprise oder Presentation Server Platinum auswählen. Sie ist nicht verfügbar, wenn Sie als Produktedition Advanced Edition ausgewählt haben.

Standardeinstellung: aktiviert bei der *Password Manager Enterprise oder Presentation Server Platinum Edition*; nicht verfügbar bei der *Password Manager Advanced Edition*

Standardeinstellung für die Verbindungstrennung: 1 Stunde, 30 Minuten bei Deaktivierung von **Lizenzverbrauch für Offlineverwendung zulassen**; 21 Tage bei Aktivierung von **Lizenzverbrauch für Offlineverwendung zulassen**

Lizenzverbrauch für Offlineverwendung zulassen

Diese Option steht nur zur Verfügung, wenn die Option **CCU-Lizenzierung** aktiviert ist. Aktivieren Sie diese Einstellung, um anzugeben, wie lange ein Benutzer im getrennten Modus (offline) sein darf, bevor die Lizenz abläuft und in den Pool der verfügbaren Lizenzen zurückgeführt wird. Wenn dieser Wert angegeben ist, behält der Benutzer während des angegebenen Zeitraums die Kontrolle über die Lizenz, auch wenn sein PC heruntergefahren wird. Standardmäßig ist ein Zeitraum von 1 Stunde und 30 Minuten eingestellt. Es sollte ein Wert zwischen 2 und 365 Tagen definiert werden.

Standardeinstellung: Nicht ausgewählt

Fortfahren ohne Prüfung der Lizenzierungsinformationen

Mit dieser Einstellung kann die Bearbeitung ohne gültigen Namen eines Lizenzservers und Ports fortgesetzt werden.

Standardeinstellung: Nicht ausgewählt

Datenschutzmethoden

Mit diesen Einstellungen werden die primären Datenschutzmethoden ausgewählt, die für den Schutz der Anmeldeinformationen der Benutzer verwendet werden.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Datenschutzmethoden

Administratorkontozugriff auf Benutzerdaten steuern

Wählen Sie **Ja** aus, wenn Administratoren nicht auf die Anmeldeinformationen der Benutzer zugreifen dürfen. Wenn Sie diese Option aktivieren, werden die Optionen unter **Microsoft Data Protection API** (einschließlich der Option **DPAPI mit Profil** im Auswahlfeld **Smartcardschlüsselquelle**) sowie die Option **Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul)** unter **Sekundäre Datenschutzmethode** deaktiviert. Mit dieser Konfiguration haben Administratoren, wie z. B. der Kontoadministrator, keinen Zugriff auf die Benutzerkennwörter oder die Benutzerdaten. Damit wird verhindert, dass ein Administrator die Identität eines Benutzers annimmt. Mit dieser Standardeinstellung kann der Administrator sich nicht als Benutzer anmelden und möglicherweise auf Daten zugreifen, die im lokalen Speicher der Anmeldeinformationen des Benutzers gespeichert sind. Wählen Sie **Nein** aus, wenn Sie die Verwendung der verschiedenen Authentifizierungsfunktionen auf dieser Seite sowie der sekundären Datenschutzmethoden unter den Konfigurationseinstellungen **Sekundäre Datenschutzmethode** ermöglichen möchten.

Standardeinstellung: Ja

Wählen Sie alle in Frage kommenden Datenschutzmethoden aus, um dem Benutzer die Anmeldung zu erleichtern.

Aktivieren Sie diese Option, um die primären Authentifizierungsfunktionen zu verwenden, die in den nachfolgenden Einstellungen aktiviert werden.

Standardeinstellung: Ausgewählt

Authentifizierungsdaten der Benutzer

Diese Einstellung ist nur verfügbar, wenn die Einstellung **Wählen Sie alle in Frage kommenden Datenschutzmethoden aus, um dem Benutzer die Anmeldung zu erleichtern** aktiviert ist. Aktivieren Sie diese Einstellung, um einen geheimen Schlüssel für die Authentifizierung zum Zugriff auf die Benutzerdaten und zu deren Schutz zu verwenden. Bei diesem Geheimnis zur Authentifizierung kann es sich um ein Benutzerkennwort oder ein PIN-basiertes Gerät in der Umgebung handeln.

Standardeinstellung: Nicht ausgewählt

Smartcard-PINs zulassen

Aktivieren Sie diese Option, um die Verwendung von Smartcard-PINs als geheimen Schlüssel für den Datenschutz zu ermöglichen. Aktivieren Sie diese Option nur, wenn das Unternehmen oder die Umgebung eine „starke PIN-Richtlinie“ hat.

Standardeinstellung: Nicht ausgewählt

Schutz mit leeren Kennwörtern zulassen

Aktivieren Sie diese Option nur, wenn die Sicherheitsanforderungen in der Domäne gering sind und die Benutzer leere Domänenkennwörter verwenden dürfen. Wenn Sie diese Option aktivieren und die Agentsoftware ein leeres Kennwort bei einem Benutzer entdeckt, wird ein nur dem Benutzer bekanntes Geheimnis aus der Benutzer-ID ermittelt. Ist diese Option nicht aktiviert, kann die Agentsoftware kein nur dem Benutzer bekanntes Geheimnis ermitteln und keine weiteren Datenschutzmaßnahmen mit dem leeren Kennwort vornehmen. Wenn Sie die Option **Authentifizierungsdaten der Benutzer** aktivieren, die Optionen **Smartcard-PINs zulassen** und **Schutz mit leeren Kennwörtern zulassen** jedoch nicht, wird eine Fehlermeldung angezeigt und die Agentsoftware wird deaktiviert, wenn ein Benutzer sich mit einem leeren Kennwort anmeldet.

Standardeinstellung: Nicht ausgewählt

Microsoft Data Protection API

Wählen Sie diese Option aus, wenn Sie servergespeicherte Profile zur Implementierung eines Kerberos-Netzwerkauthentifizierungsprotokolls für Benutzer verwenden. Diese Option funktioniert nur, wenn servergespeicherte Profile vorhanden sind. Sie können die Option **Authentifizierungsdaten der Benutzer** sowie diese Option zum Beispiel dann aktivieren, wenn die Benutzer mit Kennwörtern auf ihre PCs und mit einem Kerberos-Netzwerkauthentifizierungsprotokoll auf eine Citrix Presentation Server-Farm zugreifen. Mit dieser Methode können Benutzer sich auch mit Anmeldeinformationen und Smartcards anmelden.

Standardeinstellung: Nicht ausgewählt

Smartcardzertifikat

Aktivieren Sie diese Option, um den Benutzern die Verwendung von kryptographischen Karten zu erlauben, mit denen Authentifizierungsdaten verschlüsselt und entschlüsselt werden. Citrix empfiehlt, diese Option möglichst zu aktivieren, wenn Sie Hotdesktop mit Smartcards in der Umgebung verwenden.

Standardeinstellung: Nicht ausgewählt

Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden

Aktivieren Sie diese Option und wählen Sie aus dem Listenfeld **Smartcardschlüsselquelle** eine Methode aus, wenn die Benutzer eine primäre Authentifizierungsmethode verwenden können, und Sie die Version 4.0 oder 4.1 der Agentsoftware verwenden. Wenn Sie den zentralen Speicher von Password Manager von Version 4.1 auf Version 4.6 aktualisiert haben, ist diese Option automatisch aktiviert.

Standardeinstellung: Nicht ausgewählt

Sekundäre Datenschutzmethode

Mit diesen Optionen können Sie die Optionen für den Datenschutz mit sekundären Anmeldeinformationen festlegen, die verwendet werden, bevor die Sperre der Anmeldeinformationen des Benutzers aufgehoben wird, wenn ein Benutzer seine primäre Authentifizierung ändert (z. B. beim Ändern des Domänenkennworts oder Austauschen der Smartcard). Alternativ können Sie einstellen, dass Anmeldeinformationen automatisch wiederhergestellt werden, wenn das Modul **Schlüsselverwaltung** implementiert ist.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Sekundäre Datenschutzmethode

Benutzeridentität prüfen

Mit dieser Option geben Sie an, welche der folgenden Methoden zur Neuauthentifizierung der Benutzer verwendet werden:

- **Benutzer zur Eingabe des alten Kennworts auffordern**
- **Benutzerseitige Auswahl der Methode: Altes Kennwort oder Sicherheitsfragen**

Standardeinstellung: Ausgewählt

Benutzer zur Eingabe des alten Kennworts auffordern

Aktivieren Sie diese Option, wenn Sie möchten, dass Benutzer, die ihr Kennwort vergessen, ausgesperrt werden und sich mit den sekundären Anmeldeinformationen neu registrieren müssen. Um zu vermeiden, dass Benutzer ausgesperrt werden, sollten Sie die Self-Service-Funktion zum Zurücksetzen des Kennworts nicht ausschließlich mit der Identitätsprüfung mit dem alten Kennwort kombinieren. Wenn als Authentifizierungsmethode nur die Identitätsprüfung mit dem altem Kennwort zur Verfügung steht, werden Benutzer, die das alte primäre Kennwort vergessen, vom System ausgesperrt. Die Daten der Benutzer müssen im zentralen Speicher und auf allen Clientgeräten, auf denen sie gespeichert sind, gelöscht bzw. zurückgesetzt werden. Die Benutzer müssen die Anmeldeinformationen für alle Anwendungen neu eingeben.

Standardeinstellung: Ausgewählt

Benutzer zur Auswahl der Methode auffordern: Altes Kennwort oder Sicherheitsfragen

Aktivieren Sie diese Option, wenn die Benutzer aufgefordert werden sollen, sich mit der von ihnen ausgewählten Methode zu authentifizieren. Durch Aktivieren dieser Option wird die Option **Identitätsprüfung wie in vorherigen Password Manager-Versionen** aktiviert.

Standardeinstellung: Nicht ausgewählt

Datenschutz wie in Password Manager 4.1 und vorherigen Versionen verwenden

Aktivieren Sie diese Option, wenn Sie von Password Manager Version 4.1 aktualisieren und die fragenbasierte Authentifizierung oder Fragen zur Identitätsprüfung aktiviert ist.

Standardeinstellung: Nicht ausgewählt

Keine Aufforderung der Benutzer, primärer Datenschutz wird automatisch über das Netzwerk wiederhergestellt (benötigt das Schlüsselverwaltungsmodul)

Aktivieren Sie diese Option, wenn Sie das Schlüsselverwaltungsmodul zum Auslassen der Identitätsprüfung und zum automatischen Aufheben der Sperrung der Anmeldeinformationen der Benutzer implementieren. Diese Methode ist weniger sicher als andere Datenschutzmethoden, jedoch benutzerfreundlicher, da die Anmeldeinformationen automatisch abgerufen werden.

Standardeinstellung: Nicht ausgewählt

Self-Service-Funktionen

Für die in diesem Bereich zur Verfügung stehenden Optionen muss das Dienstmodul „Schlüsselverwaltung“ installiert werden. Dieses Modul erweitert das Windows-Anmeldedialogfeld um eine Schaltfläche, mit der die Benutzer ihre Kennwörter zurücksetzen können.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Self-Service-Funktionen

Benutzerseitiges Zurücksetzen des primären Domänenkennworts

Aktivieren Sie diese Einstellung, um die benutzerseitige Rücksetzung der Hauptdomänenkennwörter ohne Intervention des Administrators zu ermöglichen.

Standardeinstellung: Nicht ausgewählt

Benutzerseitiges Aufheben der Sperrung des Domänenkontos

Aktivieren Sie diese Einstellung, um den Benutzern zu ermöglichen, die Sperrung ihres Domänenkontos aufzuheben.

Standardeinstellung: Nicht ausgewählt

Schlüssel- verwaltungsmodul

Mit diesen Steuerelementen werden der Dienstspeicherort und der Dienstport für das Schlüsselverwaltungsmodul definiert.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Schlüsselverwaltungsmodul

Dienstspeicherort (Schlüsselverwaltungsmodul)

Mit dieser Einstellung werden die Dienstadresse und der Dienstport für das Schlüsselverwaltungsmodul definiert. Prüfen Sie mit der Schaltfläche **Wird geprüft**, ob die Einstellungen gültig sind.

Standardeinstellung: [keine Eingabe]

Dienstport: 443

Provisioningmodul

Mit dem Provisioningmodul können die Anmeldeinformationen der Benutzer in dieser Benutzerkonfiguration importiert, geändert und gelöscht werden. Auf diesen Seiten müssen Sie den Speicherort und den Dienstport des Provisioningmoduls angeben.

... Benutzerkonfigurationen > [Konfiguration] > Benutzerkonfiguration bearbeiten > Provisioningmodul

Provisioning verwenden

Aktivieren Sie diese Einstellung, um das Provisioning zu verwenden.

Standardeinstellung: Nicht ausgewählt

Dienstspeicherort (Provisioningmodul)

Mit dieser Einstellung werden die Dienstadresse und der Dienstport für das Provisioningmodul definiert. Prüfen Sie mit der Schaltfläche **Wird geprüft**, ob die Einstellungen gültig sind.

Standardeinstellung: [keine Eingabe]

Dienstport: 443

Anwendungsdefinitionen

In diesem Abschnitt werden die Einstellungen und Steuerelemente zu Anwendungsdefinitionen beschrieben. Alle Hinweise zur Navigation in diesem Abschnitt beziehen sich auf das Bearbeiten einer Anwendungsdefinition. Zum Dialogfeld **Anwendungsdefinition bearbeiten** gelangen Sie folgendermaßen:

Managementkonsolen > Access Management Console > Password Manager > Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten

Anwendungsformular bearbeiten

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Kennwortlänge und die Zeichenwiederholung gesteuert werden.

... Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungsformulare > [definiertes Formular] > Bearbeiten > Sonstige Einstellungen

Agent sendet dieses Formular automatisch

Mit dieser Einstellung wird angegeben, ob die Agentsoftware automatisch auf die Schaltfläche **Senden** klickt oder der Benutzer manuell auf die Schaltfläche **Senden** klicken muss. Aktivieren Sie das Kontrollkästchen **Agent sendet dieses Formular automatisch**, um das Formular automatisch ohne Benutzereingriff zu senden.

Standardeinstellung: Ausgewählt

Anwendungssymbol

Mit diesem Steuerelement wird das Symbol angegeben, das neben dem Anwendungsnamen im Anmeldungsmanager angezeigt wird.

... Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungssymbol

Anwendungssymbol

Mit dieser Einstellung wird das Anwendungssymbol gesteuert, das neben dem Anwendungsnamen im Anmeldungsmanager angezeigt wird. Zwei Optionen sind verfügbar:

- **Standardsymbol verwenden**
- **Benutzerdefiniertes Symbol verwenden (geben Sie den Symbolpfad unten ein)**.

Wenn Sie ein benutzerdefiniertes Symbol verwenden, können Sie den Pfad zur Symboldatei über die Funktion **Durchsuchen** angeben. Jede standardmäßige Windows-Symboldatei kann verwendet werden. Microsoft Windows-Umgebungsvariablen werden unterstützt.

Standardeinstellung: Standardsymbol verwenden

Erweiterte Erkennung

Mit diesen Steuerelementen wird die Agentsoftware gezwungen, nachfolgende Formulare für die Anmeldung oder die Kennwortänderung in einer Anwendungssitzung zu ignorieren, wenn eine Anmeldung oder Kennwortänderung bereits verarbeitet wurde.

... Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Anwendungserkennung

Nur die erste Anmeldung für diese Anwendung verarbeiten

Aktivieren Sie dieses Steuerelement, wenn nur die erste Anmeldung für diese Anwendung verarbeitet werden soll und nachfolgende Anmeldeanfragen ignoriert werden sollen.

Standardeinstellung: Nicht ausgewählt

Nur die erste Kennwortänderung für diese Anwendung verarbeiten

Aktivieren Sie dieses Steuerelement, wenn nur die erste Kennwortänderungsanfrage für diese Anwendung verarbeitet werden soll und nachfolgende Kennwortänderungsanfragen ignoriert werden sollen.

Standardeinstellung: Nicht ausgewählt

Kennwortablauf

Mit diesen Steuerelementen werden die Einstellungen zum Kennwortablauf für diese Anwendung festgelegt. Das Einhalten der Ablaufrichtlinie von Citrix Password Manager wird nur erzwungen, wenn sie in der Kennwortrichtlinie aktiviert ist, die dieser Anwendung zugeordnet ist.

... Anwendungsdefinitionen > [Definition] > Anwendungsdefinition bearbeiten > Kennwortablauf

Bei Kennwortablauf Skript ausführen

Aktivieren Sie diese Einstellung und geben Sie ein Skript und dessen Pfad an, wenn beim Ablauf des Kennworts eine bestimmte Skriptdatei ausgeführt werden soll. Weitere Informationen finden Sie unter “Kennwortablauf konfigurieren“ auf Seite 56.

Standardeinstellung: Nicht ausgewählt

Citrix Password Manager-Ablaufwarnung verwenden

Aktivieren Sie diese Einstellung, um die Citrix Password Manager-Ablaufwarnung zu verwenden, wenn ein Kennwort abläuft. Weitere Informationen finden Sie unter “Kennwortablauf konfigurieren“ auf Seite 56.

Standardeinstellung: Nicht ausgewählt

Kennwortrichtlinien

In diesem Abschnitt werden die Einstellungen und Steuerelemente zu Kennwortrichtlinien beschrieben. Alle Hinweise zur Navigation in diesem Abschnitt beziehen sich auf das Bearbeiten einer vorhandenen Kennwortrichtlinie. Zum Dialogfeld **Kennwortrichtlinie bearbeiten** gelangen Sie folgendermaßen:

Managementkonsolen > Access Management Console > Password Manager > Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten

Grundlegende Kennwortregeln

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Kennwortlänge und die Zeichenwiederholung gesteuert werden.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Grundlegende Kennwortregeln

Mindestlänge für Kennwort

Gibt die Mindestanzahl der Zeichen für ein Kennwort an. Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 8

Höchstlänge für Kennwort

Gibt das Maximum der Zeichen für ein Kennwort an. Mindestwert = 1, Höchstwert =128.

Standardeinstellung: 20

Höchstanzahl wiederholter Zeichen

Gibt an, wie oft ein Zeichen in einem Kennwort wiederholt werden kann. Mindestwert = 1, Höchstwert =128.

Standardeinstellung: 6

Höchstanzahl aufeinanderfolgender gleicher Zeichen

Gibt die Höchstanzahl aufeinanderfolgender gleicher Zeichen an. Mindestwert = 1, Höchstwert =128.

Standardeinstellung: 4

Regeln für Buchstaben

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Buchstaben in Kennwörtern gesteuert wird.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Buchstaben

Kleinbuchstaben zulassen

Steuert, ob Kleinbuchstaben in Kennwörtern zulässig sind.

Standardeinstellung: Kleinbuchstaben zulassen

Erstes Zeichen im Kennwort kann Kleinbuchstabe sein

Steuert, ob Kennwörter mit einem Kleinbuchstaben beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Kleinbuchstabe sein

Letztes Zeichen im Kennwort kann Kleinbuchstabe sein

Steuert, ob Kennwörter mit einem Kleinbuchstaben enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Ziffer sein

Mindestanzahl der Kleinbuchstaben:

Gibt die Mindestanzahl der Kleinbuchstaben in einem Kennwort an. Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 0

Großbuchstaben zulassen

Steuert, ob Großbuchstaben in Kennwörtern zulässig sind.

Standardeinstellung: Großbuchstaben zulassen

Erstes Zeichen im Kennwort kann Großbuchstabe sein

Steuert, ob Kennwörter mit einem Großbuchstaben beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Großbuchstabe sein

Letztes Zeichen im Kennwort kann Großbuchstabe sein

Steuert, ob Kennwörter mit einem Großbuchstaben enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Großbuchstabe sein

Mindestanzahl der Großbuchstaben

Gibt die Mindestanzahl der Großbuchstaben in einem Kennwort an. Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 0

Regeln für Ziffern

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Ziffern (0 bis 9) in Kennwörtern gesteuert wird.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Ziffern

Ziffern zulassen

Steuert, ob Ziffern in Kennwörtern zulässig sind.

Standardeinstellung: Sonderzeichen zulassen

Erstes Zeichen im Kennwort kann Ziffer sein

Steuert, ob Kennwörter mit einer Ziffer beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Ziffer sein

Letztes Zeichen im Kennwort kann Ziffer sein

Steuert, ob Kennwörter mit einer Ziffer enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Ziffer sein

Mindestanzahl der Ziffern

Gibt die Mindestanzahl der Ziffern in einem Kennwort an.
Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 0

Höchstanzahl der Ziffern

Gibt die Höchstanzahl der Ziffern in einem Kennwort an.
Mindestwert = 1, Höchstwert =128.

Standardeinstellung: 20

Regeln für Sonderzeichen

Mit diesen Steuerelementen werden die Regeln festgelegt, mit denen die Verwendung von Sonderzeichen (keine Buchstaben und Ziffern) in Kennwörtern festgelegt wird.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Regeln für Sonderzeichen

Sonderzeichen zulassen

Steuert, ob Sonderzeichen (keine Buchstaben und Ziffern) in Kennwörtern zulässig sind.

Standardeinstellung: Sonderzeichen zulassen

Erstes Zeichen im Kennwort kann Sonderzeichen sein

Steuert, ob Kennwörter mit einem Sonderzeichen beginnen können.

Standardeinstellung: Erstes Zeichen im Kennwort kann Sonderzeichen sein

Letztes Zeichen im Kennwort kann Sonderzeichen sein

Steuert, ob Kennwörter mit einem Sonderzeichen enden können.

Standardeinstellung: Letztes Zeichen im Kennwort kann Sonderzeichen sein

Mindestanzahl der Sonderzeichen

Gibt die Mindestanzahl der Sonderzeichen in einem Kennwort an.
Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 0

Höchstanzahl der Sonderzeichen

Gibt die Höchstzahl der Sonderzeichen in einem Kennwort an.
Mindestwert = 0, Höchstwert =128.

Standardeinstellung: 20

Liste zulässiger Sonderzeichen

Gibt die für Kennwörter zulässigen Sonderzeichen an.

Standardeinstellung: `!@#$^&*()_-+=[]\|,?`

Ausschlussregeln

Mit diesen Steuerelementen werden die Zeichen und Zeichenfolgen angegeben, die für Kennwörter nicht zulässig sind.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Ausschlussregeln

Folgende Liste der Zeichen oder Zeichengruppen von Kennwörtern ausschließen

Wählen Sie die Option **Liste bearbeiten** aus, um das Dialogfeld **Ausschlussliste bearbeiten** zu öffnen. Dort können Sie bis zu 256 Zeichen oder Zeichengruppen angeben, die für Kennwörter nicht zulässig sein sollen. Geben Sie ein Zeichen oder eine Zeichengruppe pro Zeile ein. Jede Gruppe kann maximal 32 Zeichen enthalten. Bei Zeichen und Zeichengruppen wird die Groß- und Kleinschreibung nicht beachtet.

Standardeinstellung: [keine Eingabe]

Anwendungsbenutzername im Kennwort nicht zulassen

Steuert, ob der Anwendungsbenutzername im Kennwort zulässig ist. Aktivieren Sie dieses Kontrollkästchen, wenn der Anwendungsbenutzername im Kennwort nicht zulässig ist.

Standardeinstellung: Nicht ausgewählt

Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen

Steuert, ob Teile des Anwendungsbenutzernamens im Kennwort zulässig sind. Dies umfasst alle Zeichengruppen, die vom Benutzernamen verwendet werden können. Diese Einstellung ist mit der Einstellung **Zeichenanzahl in Teilen** gekoppelt. Beispiel: Wenn diese Einstellung aktiviert ist und **Zeichenanzahl in Teilen** auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen „citrix" kein Kennwort mit den Zeichenfolgen „citr", „itri" oder „trix" verwenden.

Standardeinstellung: Nicht ausgewählt

Zeichenanzahl in Teilen

Definiert die Länge der Zeichenfolge, die als Teil eines Kennworts untersucht werden muss, um festzustellen, ob das angegebene Kennwort einen Teil des Anwendungsbenutzernamens enthält. Beispiel: Wenn die Option **Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen** aktiviert ist und diese Einstellung auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen „citrix" kein Kennwort mit den Zeichenfolgen „citr", „itri" oder „trix" verwenden.

Standardeinstellung: 3

Windows-Benutzername im Kennwort nicht zulassen

Steuert, ob der Anwendungsbenutzername im Kennwort zulässig ist. Wenn diese Einstellung nicht aktiviert ist, ist der Windows-Benutzername im Kennwort zulässig.

Standardeinstellung: Nicht ausgewählt

Teile des Windows-Benutzernamens im Kennwort nicht zulassen

Steuert, ob Teile des Windows-Benutzernamens des Benutzers im Kennwort zulässig sind. Dies umfasst alle Zeichengruppen, die vom Benutzernamen verwendet werden können. Diese Einstellung ist mit der Einstellung **Zeichenanzahl in Teilen** gekoppelt. Beispiel: Wenn diese Einstellung aktiviert ist und **Zeichenanzahl in Teilen** auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen „citrix" kein Kennwort mit den Zeichenfolgen „citr", „itri" oder „trix" verwenden.

Standardeinstellung: Teile zugelassen (Kontrollkästchen nicht aktiviert)

Zeichenanzahl in Teilen

Definiert die Länge der Zeichenfolge, die als Teil eines Kennworts untersucht werden muss, um festzustellen, ob das angegebene Kennwort einen Teil des Anwendungsbenutzernamens enthält. Beispiel: Wenn die Option Teile des Anwendungsbenutzernamens im Kennwort nicht zulassen aktiviert ist und diese Einstellung auf vier festgelegt ist, darf ein Benutzer mit dem Benutzernamen „citrix“ kein Kennwort mit den Zeichenfolgen „citr“, „itri“ oder „trix“ verwenden.

Standardeinstellung: 3

Kennwortverlauf und -ablauf

Diese Steuerelemente legen fest, ob ein neues Kennwort mit einem alten Kennwort identisch sein darf. Außerdem legen sie die Einstellungen zum Kennwortablauf fest.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Kennwortverlauf und -ablauf

Neues Kennwort darf nicht mit den alten Kennwörtern identisch sein

Steuert, ob das neue Kennwort mit einem der alten Kennwörter identisch sein darf. Die alten Kennwörter werden im Kennwortverlauf gespeichert.

Standardeinstellung: Neues Kennwort darf mit altem Kennwort identisch sein (Kontrollkästchen nicht aktiviert)

Anzahl der gespeicherten alten Kennwörter

Gibt die Anzahl alter Kennwörter an, die im Kennwortverlauf gespeichert sind. Mindestwert = 1, Höchstwert = 24

Standardeinstellung: 1

Kennwortablauf

Wenn diese Einstellung aktiviert ist, werden die definierten Einstellungen **Anzahl der Tage bis zum Ablauf des Kennworts** und **Anzahl der Tage für Hinweis der Benutzer auf Kennwortablauf** auf die Anwendungsdefinitionen angewendet, denen diese Richtlinie zugeordnet ist. Die Richtlinie von Citrix Password Manager funktioniert unabhängig von vorhandenen Kennwortablaufrichtlinien, die in die Anwendung integriert sind.

Standardeinstellung: Kennwortablauf nicht festgelegt (Kontrollkästchen nicht aktiviert)

Anzahl der Tage bis zum Ablauf des Kennworts

Gibt die maximale Anzahl der Tage an, für die ein Kennwort nicht geändert werden muss. Mindestwert = 1, Höchstwert = 99999

Standardeinstellung: 42

Anzahl der Tage für Hinweis der Benutzer auf Kennwortablauf

Gibt an, ab wie vielen Tagen vor dem Ablauf eines Kennworts ein Benutzer Hinweise auf den Kennwortablauf erhält. Mindestwert = 0, Höchstwert = 99998

Standardeinstellung: 14

Kennwortrichtlinie testen

Mit diesen Steuerelementen kann ein manuell generiertes Kennwort auf die Kompatibilität mit der definierten Richtlinie überprüft werden, automatisch ein mit der Richtlinie kompatibles Kennwort generiert werden und geprüft werden, ob mit den festgelegten Einschränkungen genügend Kennwörter für das Unternehmen generiert werden können.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Kennwortrichtlinie testen

Regeleinhaltung eines manuell erstellten Kennworts testen

Mit diesem Feld kann die Regeleinhaltung eines manuell erstellten Kennworts getestet werden. Geben Sie das manuell erstellte Kennwort ein und klicken Sie auf **Testen**. Das eingegebene Kennwort wird anhand aller definierten Kriterien überprüft.

Standardeinstellung: Keine

Regelkompatibles, willkürliches Kennwort erstellen

Mit diesem Steuerelement wird ein Kennwort generiert, das die aktuell definierten Kennwortkriterien erfüllt. Klicken Sie auf **Erstellen**, um ein regelkompatibles Kennwort zu generieren, das aus dem Feld kopiert werden kann (Strg+C).

Standardeinstellung: Keine

Mehrere eindeutige, regelkompatible Kennwörter erstellen und testen

Es kann vorkommen, dass die festgelegten Einschränkungen für Kennwörter dazu führen, dass nicht mehr genügend Kennwörter möglich sind. Mit diesem Steuerelement wird eine benutzerdefinierte Anzahl von regelkompatiblen Kennwörtern generiert, um zu ermitteln, ob die definierte Richtlinie flexibel genug ist, um den Anforderungen des Unternehmens in Bezug auf Kennwörter gerecht werden zu können. Klicken Sie auf **Mehrere Kennwörter erstellen**, um ein Dialogfeld zu öffnen, in dem Sie eine benutzerdefinierte Anzahl von Kennwörtern generieren können.

Standardeinstellung: Keine

Anmeldeeinstellungen

Mit diesen Steuerelementen wird definiert, ob die Option **Anzeigen** für Anwendungsdefinitionen verfügbar ist, die diese Richtlinie verwenden, ob sich die Benutzer vor dem Senden der Anwendungsanmeldeinformationen neu authentifizieren müssen, und wie lange ein Benutzer nach einer fehlgeschlagenen Authentifizierung erneut versuchen darf, sich zu authentifizieren.

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Anmeldeeinstellungen

Benutzer können Kennwort für Anwendungen anzeigen

Mit diesem Steuerelement wird festgelegt, ob die Schaltfläche **Anzeigen** für die Anwendungen, denen diese Richtlinie zugeordnet ist, im Anmeldungsmanager zur Verfügung steht. Wenn die Benutzer im Anmeldungsmanager auf **Anzeigen** klicken, wird das Kennwort in Klartext angezeigt. Wenn diese Einstellung nicht aktiviert ist, können die Benutzer die Kennwörter nicht anzeigen.

Standardeinstellung: Schaltfläche **Anzeigen** nicht verfügbar (Kontrollkästchen nicht aktiviert)

Neue Benutzerauthentifizierung vor dem Senden der Anwendungsanmeldeinformationen erzwingen

Mit diesem Steuerelement wird festgelegt, ob die Benutzer ihre primären Anmeldeinformationen eingeben müssen, bevor der Agent die Anmeldeinformationen an die Anwendung sendet. Wenn diese Einstellung aktiviert ist, sperrt der Agent die Arbeitsstation sofort, wenn er eine Anwendung erkennt, die von dieser Einstellung verwaltet wird. Benutzer müssen die primären Anmeldeinformationen eingeben, um die Sperrung der Arbeitsstation aufzuheben. Wenn die Sperrung der Arbeitsstation mit den richtigen Anmeldeinformationen aufgehoben wird, sendet der Agent die Anmeldeinformationen des Benutzers an die Anwendung. Diese Einstellung ist für Anwendungen nützlich, die auf vertrauliche Informationen zugreifen, da die Prüfung der Benutzeridentität erzwungen wird, bevor der Agent die Anmeldeinformationen an die Anwendung sendetgezwungen.

Standardeinstellung: Benutzer müssen sich nicht neu authentifizieren (Kontrollkästchen ist nicht aktiviert)

Anzahl der Anmeldewiederholungsversuche

Mit diesem Steuerelement wird festgelegt, wie oft der Agent in der angegebenen Zeitspanne die Anmeldeinformationen eines Benutzers erneut an dieselbe Anwendung senden kann. Wenn diese Einstellung auf den Mindestwert von 0 eingestellt ist, erhalten Benutzer sofort beim zweiten versuchten Senden der Anmeldeinformationen an die Anwendung eine Fehlermeldung.

Standardeinstellung: 1

Zeitlimit für Wiederholungsversuche

Mit diesem Steuerelement wird festgelegt, über welchen Zeitraum (in Sekunden) ein Benutzer seine Anmeldeinformationen erneut an dieselbe Anwendung senden darf, wenn das erste Senden der Anmeldeinformationen fehlgeschlagen ist.

Standardeinstellung: 30 Sekunden

Assistent für Kennwortänderungen

Mit diesem Steuerelement wird festgelegt, wie der Assistent für Kennwortänderungen auf Kennwortänderungsformulare antwortet. Eine der vier zur Auswahl stehenden Optionen muss aktiviert werden.

- Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen
- Benutzer können nur ein eigenes Kennwort erstellen
- Benutzer können nur ein systemgeneriertes Kennwort auswählen
- Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden

... Kennwortrichtlinien > [Richtlinie] > Kennwortrichtlinie bearbeiten > Assistent für Kennwortänderungen

Benutzer können ein systemgeneriertes Kennwort auswählen oder ein eigenes erstellen

Aktivieren Sie diese Option, wenn die Benutzer im Assistenten für Kennwortänderungen die Wahl zwischen einem systemgenerierten Kennwort und dem Erstellen eines eigenen haben sollen.

Standardeinstellung: Ausgewählt

Benutzer können nur ein eigenes Kennwort erstellen

Aktivieren Sie diese Option, wenn die Benutzer im Assistenten für Kennwortänderungen kein systemgeneriertes Kennwort auswählen können, sondern ein eigenes erstellen sollen.

Standardeinstellung: Nicht ausgewählt

Benutzer können nur ein systemgeneriertes Kennwort auswählen

Aktivieren Sie diese Option, wenn der Assistent für Kennwortänderungen automatisch ein systemgeneriertes Kennwort verwenden soll und die Benutzer keine eigenen Kennwörter erstellen dürfen.

Standardeinstellung: Nicht ausgewählt

Kennwort erstellen und ohne Anzeigen des Assistenten an die Anwendung senden

Aktivieren Sie diese Option, wenn die Agentsoftware automatisch ein systemgeneriertes Kennwort senden und den Benutzern nicht den Assistenten für Kennwortänderungen anzeigen soll. Der Benutzer sieht möglicherweise im Dialogfeld für die Kennwortänderung, dass die Felder eingegeben werden. Die Anwendung zeigt dann an, ob die Kennwortänderung erfolgreich war.

Standardeinstellung: Nicht ausgewählt

Erweiterungen von Anwendungsdefinitionen

Obwohl Anwendungsdefinitionen von Password Manager-Administratoren in der Regel in der Password Manager Console und im Anwendungsdefinitionstool erstellt werden, ist für einige Anwendungen aufgrund spezieller Anforderungen ein externer Prozess erforderlich, um zu überprüfen, ob eine Anwendung gestartet wurde oder um Anmeldeinformationen mit der Agentsoftware zu senden.

Implementierer von Drittanbietern, die für diese Anwendungen entsprechende externe Prozesse erstellen, können dabei mit den Erweiterungen von Anwendungsdefinitionen in der Password Manager Console und dem Anwendungsdefinitionstool festlegen, wann und wie diese Prozesse initiiert werden.

In diesem Anhang wird beschrieben, wie diese Erweiterungen konfiguriert werden. In diesem Anhang wird nicht beschrieben, wie die externen Prozesse definiert oder erstellt werden, um zu bestimmen, ob eine Anwendung gestartet wurde oder um Anmeldeinformationen mit der Agentsoftware zu senden.

Agentsoftwarevorgänge

Es gibt zwei verschiedene Typen der Erweiterungen von Anwendungsdefinitionen:

- Identifizierungserweiterungen

  Verwenden von externen Prozessen zum Prüfen, ob es sich bei der Zielanwendung um ein Formular handelt, für das Aktionen zum Verwalten von Anmeldeinformationen von Benutzern erforderlich sind. Diese externen Prozesse können statt oder zusammen mit anderen Fenstererkennungsalgorithmen verwendet werden, die in der Formulardefinition festgelegt sind.

- Aktionserweiterungen

  Verwenden von externen Prozessen zum Ausführen der erforderlichen Aktionen zum Verwalten von Anmeldeinformationen des Benutzers. Diese externen Prozesse können statt oder zusammen mit anderen Fensteraktionsalgorithmen verwendet werden, die in der Formulardefinition festgelegt sind.

Eine Formulardefinition kann so konfiguriert werden, dass Erweiterungen von Anwendungsdefinitionen verwendet werden, um jeweils einen oder beide Vorgänge damit durchzuführen.

Identifizierungserweiterungen

Die Agentsoftware ermittelt mit Listenerhooks Ereignisse auf dem Desktop, z. B. Anwendungsinstanziierung, Laden von URLs, Hinweise zur Vollständigkeit von Dokumenten bei HTML-Seiten und andere ähnliche Ereignisse.

Wenn diese Ereignisse auftreten, prüft die Agentsoftware, ob für die Zielanwendung eine Aktion zum Verwalten von Ameldeinformationen des Benutzers (z. B. Ignorieren, Anmelden, Kennwort ändern usw.) erforderlich ist. Dafür werden die Merkmale einer Anwendung mit den definierten Merkmalen verglichen, die ein Formular eindeutig identifizieren. Dazu gehören (als Mindestangaben) der Windows-Titel und der Name der ausführbaren Datei sowie bei Bedarf andere erweiterte Zuordnungsmerkmale, z. B. das Verwenden eines externen Prozesses zur Formularidentifizierung (*Identifizierungserweiterung*).

Bei einer erforderlichen externen Identifizierung werden der oder die zugehörigen Prozesse in der Formulardefinition angegeben. Die Formulardefinition enthält Angaben zur Identifizierungserweiterung und zu allen zugehörigen Parametern. Diese beziehen sich direkt auf eine Einstellung in der Registrierung.

Nach dem Verarbeiten der Mindest- und der erweiterten Zuordnungsalgorithmen durch die Agentsoftware werden Identifizierungserweiterungen geprüft, die einen externen Prozess erfordern.

Wenn mehrere Identifizierungserweiterungen für das Prüfen eines Formulars definiert sind, werden die Erweiterungen in der Reihenfolge ausgeführt, in der sie auf der Seite der Identfizierungserweiterungen angezeigt sind (von oben nach unten).

Für jede Identifizierungserweiterung bleibt die Agentsoftware die festgelegte Zeitdauer inaktiv (definiert in der Registrierungseinstellung), um auf das Beenden des externen Prozesses zu warten und im Anschluss den Prozessbeendigungscode zu analysieren.

Wenn die Prozesse für Mindestzuordnung, erweiterte Zuordnung und externe Zuordnung mit einem Rückgabecode von null abgeschlossen werden, wird die Zielanwendung als Übereinstimmung angesehen. Wenn ein Zuordnungsprozess mit einem anderen Wert beendet wird, wird der Auswertungsprozess beendet, und die Anwendung wird nicht als Übereinstimmung angesehen.

Bei einem negativen Rückgabewert wird in der Windows-Ereignisanzeige ein Fehler protokolliert. Positive Werte werden in eine Protokolldatei eingetragen. (Weitere Informationen finden Sie unter „Aktivieren der Protokollierung“ auf Seite 324.)

Die folgende Aktion zum Verwalten von Anmeldeinformationen des Benutzers kann über eine beliebige Kombination von standardmäßigen Windows-Formularaktionen, Aktionsfolgen oder Aktionserweiterungen durchgeführt werden. (Weitere Informationen finden Sie unter „Aktionserweiterungen“ auf Seite 319.) Zusätzliche Informationen finden Sie unter „Formularaktionen definieren“ auf Seite 64 oder „Definieren der Aktionsfolge für Formulare mit dem Aktionseditor“ auf Seite 74.

Definieren von Identifizierungserweiterungen

Identifizierungserweiterungen werden mit dem Assistenten für Formulardefinitionen beim Entwickeln der Anwendungsdefinition konfiguriert. (Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick“ auf Seite 53 und „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.)

So definieren Sie eine Identifizierungserweiterung

1. Starten Sie den Assistenten für Formulardefinitionen. (Weitere Informationen finden Sie unter „Assistent für Formulardefinitionen im Überblick“ auf Seite 57.)
2. Durchlaufen Sie den Definitionsprozess, bis die Seite **Formular identifizieren** angezeigt wird. (Weitere Informationen finden Sie unter „Formular identifizieren“ auf Seite 86.)
3. Klicken Sie auf der Seite **Formular identifizieren** auf **Erweiterte Zuordnung**. Im Anschluss wird das Dialogfeld **Erweiterte Zuordnung** angezeigt. (Weitere Informationen finden Sie unter „Verwenden der erweiterten Zuordnung zum Identifizieren von Windows-Formularen“ auf Seite 67.)
4. Wählen Sie im Dialogfeld **Erweiterte Zuordnung** die Option **Identifizierungserweiterungen** aus. Die Seite **Identifizierungserweiterungen** wird angezeigt. Auf dieser Seite können Identifizierungserweiterungseinträge angezeigt, bearbeitet oder hinzugefügt werden.
5. Klicken Sie auf **Hinzufügen**, um eine Identifizierungserweiterung hinzuzufügen. Dadurch wird das Dialogfeld **Identifizierungserweiterungen hinzufügen** geöffnet. Im Dialogfeld **Identifizierungserweiterungen hinzufügen** definieren Sie Folgendes:

Erweiterungs-ID	Die Erweiterungs-ID kennzeichnet den *ExtensionName*, nach dem in den Registrierungseinstellungen gesucht werden soll.
Beschreibung	Eine benutzerdefinierte Beschreibung der zu definierenden Identifizierungserweiterung.
Parameter	Ein beliebiges Name/Wert-Paar (Parametername/ Parameterwert), mit dem vom Implementierer definierte Parameter an den externen Prozess übertragen werden, der von dieser Erweiterung gestartet wird.

Der *ExtensionName* gibt den Namen eines Registrierungsschlüssels an. Der Schlüsselname und die ihm zugeordneten Schlüsselwerte definieren die ausführbare Datei für den externen Identifizierungsprozess und die zugehörigen Verwendungsmerkmale. Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Dabei wird der Wert für *ExtensionName* über den Wert der Erweiterungs-ID im Dialogfeld **Identifizierungserweiterung hinzufügen** identifiziert.

Auf 64-Bit-Plattformen befinden sich der Name des Registrierungsschlüssels und die zugeordneten Schlüssel unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix \MetaFrame Password Manager\Extension\{ExtensionName}]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Schlüssel	Typ	Wert
Type	REG_SZ	Muss EXECUTABLE sein.
Timeout	REG_DWORD	0, um ohne Timeout auf das Beenden der Anwendung zu warten. Jeder andere Wert gibt die Wartezeit in Millisekunden an.
TerminateProcess	BOOL implementiert als REG_DWORD	(optional) Prozess bei Timeout beenden. TRUE: (Standard) Prozess beenden. FALSE: (0) Prozess nicht beenden.
Executable	REG_EXPAND_SZ	Der ausführbare Prozess und der vollqualifizierter Pfad.
Arguments	REG_SZ	Parameter für die ausführbare Datei.

Der Wert für *Executable* gibt den vollständigen Pfad zur ausführbaren Datei an. Umgebungsvariablen sind zulässig. Wenn die Erweiterung als Skript implementiert wird, muss der Skript-Interpreter für *Executable* und der Skriptname als Teil von *Arguments* verwendet werden. Externe Prozesse können mit Editoren/Sprachen oder IDEs Ihrer Wahl entwickelt werden.

Der Wert *Arguments* unterstützt Parameter, die von der Agentsoftware durch Echtzeitparameter oder durch die Parametername/Wert-Paare, die im Dialogfeld **Identifizierungserweiterungen hinzufügen** festgelegt wurden, ersetzt werden können. Jeder zu ersetzende Parameter benötigt als Trennzeichen ein $ (Dollarzeichen) als Präfix und Suffix. Ein Beispiel für *Befehlszeilenargumente*:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

Diese Befehlszeilenargumente werden von der ausführbaren Datei folgendermaßen interpretiert:

```
/h 1275366 /s "Houston, TX" /t 43
```

Der der Anwendung zugeordnete Handle von Microsoft Windows ist ein unterstützter interner Parameter, der als $_HANDLE$ definiert ist.

Alle internen Parameter verwenden $_ als Präfix, um Benennungskonflikte zu vermeiden. Implementiererparameter dürfen keine Unterstreichungszeichen in Schlüsselnamen haben.

Die Ersetzungspriorität ist festgelegt, damit die Parameterwerte nach dem Schreiben erhalten bleiben. Die Priorität ist definiert als interne Parameter (z. B. $_HANDLE$), gefolgt von Implementiererparametern, gefolgt von Umgebungsvariablen.

Für alle Implementiererparameter können Groß- und Kleinbuchstaben und Ziffern in Schlüsselnamen verwendet werden. Bei den Schlüsselnamen braucht nicht auf die Groß- bzw. Kleinschreibung geachtet zu werden.

Wenn durch die ausführbare Datei der Erweiterungsidentifizierung festgelegt ist, dass Parameter in einer bestimmten Reihenfolge aufgerufen werden müssen, muss *Argument* die erforderliche Reihenfolge unterstützen. Parameternamen/Wert-Paare im Dialogfeld **Identifizierungserweiterungen hinzufügen** können in einer beliebigen Reihenfolge definiert sein.

Aktionserweiterungen

Aktionserweiterungen verwalten Aktionen zur Verwaltung von Anmeldeinformationen des Benutzers mit einem externen Prozess. Mit dem Erweiterungsdefinitionsprozess können Anmeldeinformationen des Benutzers an die externe Anwendung übertragen werden.

Nachdem ein Formular zum Verwalten von Anmeldeinformationen des Benutzers erfolgreich identifiziert wurde (siehe „Identifizierungserweiterungen" auf Seite 314) kann die folgende Aktion zum Verwalten von Anmeldeinformationen des Benutzers über eine beliebige Kombination von standardmäßigen Windows-Formularaktionen, Aktionsfolgen oder Aktionserweiterungen durchgeführt werden.

Die Agentsoftware unterstützt dieselben unter „Identifizierungserweiterungen" auf Seite 314 beschriebenen Funktionen.

Die Agentsoftware führt den externen Prozess aus und bleibt dann für den festgelegten Zeitraum inaktiv (wenn für *WaitForCompletion* der Wert TRUE festgelegt ist), um auf das Ende des externen Prozesses zu warten und im Anschluss den Prozessbeendigungscode zu analysieren. Wenn der Prozess mit einem Rückgabewert von null beendet wird, wurde die Erweiterung erfolgreich ausgeführt. Ein Rückgabewert ungleich null verweist auf einen Fehler.

Bei einem negativen Wert wird der Fehler in der Windows-Ereignisanzeige protokolliert. Positive Werte werden in eine Protokolldatei eingetragen. (Weitere Informationen finden Sie unter „Aktivieren der Protokollierung" auf Seite 324.)

Definieren von Aktionserweiterungen

Aktionserweiterungen werden mit dem Assistenten für Formulardefinitionen beim Entwickeln der Anwendungsdefinition konfiguriert. (Weitere Informationen finden Sie unter „Assistent für Anwendungsdefinitionen im Überblick" auf Seite 53 und „Assistent für Formulardefinitionen im Überblick" auf Seite 57.)

So definieren Sie eine Aktionserweiterung

1. Starten Sie den Assistenten für Formulardefinitionen. (Weitere Informationen finden Sie unter „Assistent für Formulardefinitionen im Überblick" auf Seite 57.)
2. Durchlaufen Sie den Definitionsprozess, bis die Seite **Formularaktionen definieren** angezeigt wird. (Weitere Informationen finden Sie unter „Formularaktionen definieren" auf Seite 64.)
3. Klicken Sie auf der Seite **Formularaktionen definieren** auf **Aktionseditor...**. Das Dialogfeld **Aktionseditor** wird geöffnet (siehe „Definieren der Aktionsfolge für Formulare mit dem Aktionseditor" auf Seite 74).

4. Wählen Sie im Dialogfeld **Aktionseditor...** die Option **Aktionserweiterung starten** aus. Das Feld **Aktionskonfiguration** wird angezeigt. In diesem Feld können Sie Aktionsfolgeeinträge für **Aktionserweiterung starten** anzeigen, bearbeiten oder hinzufügen.

5. Geben Sie die folgenden Informationen ein und klicken Sie auf **Einfügen**, um einer Aktionsfolge eine Aktionserweiterung hinzuzufügen:

Erweiterungs-ID	Die Erweiterungs-ID kennzeichnet den *ExtensionName*, nach dem in den Registrierungseinstellungen gesucht werden soll.
Beschreibung	Eine benutzerdefinierte Beschreibung der zu definierenden Aktionserweiterung.
Parameter	Ein beliebiges Name/Wert-Paar (Parametername/Parameterwert), mit dem vom Implementierer definierte Parameter an den externen Prozess gesendet werden, der von dieser Erweiterung gestartet wird.

Wie bei den Identifizierungserweiterungen kennzeichnet *ExtensionName* den Namen eines Registrierungsschlüssels. Der Schlüsselname und die ihm zugeordneten Schlüsselwerte definieren die ausführbare Datei für den externen Identifizierungsprozess und die zugehörigen Verwendungsmerkmale. Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

Dabei wird der Wert für *ExtensionName* über den ID-Wert im Feld **Aktionskonfiguration** identifiziert.

Auf 64-Bit-Plattformen befinden sich der Name des Registrierungsschlüssels und die zugeordneten Schlüssel unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\MetaFrame Password Manager\Extension\{ExtensionName}]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Taste	Typ	Wert
Type	REG_SZ	Muss EXECUTABLE sein.
Timeout	REG_DWORD	0, um ohne Timeout auf das Beenden der Anwendung zu warten. Jeder andere Wert gibt die Wartezeit in Millisekunden an.
TerminateProcess	BOOL implementiert als REG_DWORD	(optional) Prozess bei Timeout beenden. TRUE: (Standard) Prozess beenden. FALSE: (0) Prozess nicht beenden.
WaitForCompletion	BOOL implementiert als REG_DWORD	(optional) Agent wartet auf Beenden des Prozesses. TRUE: (Standard) Warten. FALSE: (0) Nicht warten.
Executable	REG_EXPAND_SZ	Der ausführbare Prozess und der vollqualifizierte Pfad.
Arguments	REG_SZ	Parameter für die ausführbare Datei.

Für den Wert für *Executable* gelten dieselben Konventionen wie für die Identifizierungserweiterungen.

Der Wert *Arguments* unterstützt Parameter, die von der Agentsoftware durch Echtzeitparameter oder durch die Parametername/Wert-Paare, die in der Ansicht **Aktionserweiterung starten** des Aktionseditors festgelegt wurden, ersetzt werden können. Jeder zu ersetzende Parameter benötigt als Trennzeichen ein $ (Dollarzeichen) als Präfix und Suffix. Ein Beispiel für *Befehlszeilenargumente*:

```
/h $_HANDLE$ /s $SAPSERVER$ /t $SAPTYPE$
```

Diese Befehlszeilenargumente werden von der ausführbaren Datei folgendermaßen interpretiert:

```
/h 1275366 /s "Houston, TX" /t 43
```

Der der Anwendung zugeordnete Handle von Microsoft Windows ist ein unterstützter interner Parameter, der als $_HANDLE$ definiert ist.

Alle internen Parameter verwenden $_ als Präfix, um Benennungskonflikte zu vermeiden. Implementiererparameter dürfen keine Unterstreichungszeichen in Schlüsselnamen haben.

Zusätzlich zum Windows-Handle werden die folgenden internen Parameter zum Verwalten von Anmeldeinformationen unterstützt:

- Benutzername: $_USERNAME$
- Kennwort: $_PASSWORD$
- Benutzerdefiniert 1: $_CUSTOM1$
- Benutzerdefiniert 2: $_CUSTOM2$
- Altes Kennwort: $_OLDPASSWORD$

Die Ersetzungspriorität ist festgelegt, damit die Parameterwerte nach dem Schreiben erhalten bleiben. Die Priorität ist definiert als interne Parameter, gefolgt von Implementiererparametern, gefolgt von Umgebungsvariablen.

Für alle Implementiererparameter können Groß- und Kleinbuchstaben und Ziffern in Schlüsselnamen verwendet werden. Bei den Schlüsselnamen braucht nicht auf die Groß- bzw. Kleinschreibung geachtet zu werden.

Wenn durch die ausführbare Datei der Erweiterungsidentifizierung festgelegt ist, dass Parameter in einer bestimmten Reihenfolge aufgerufen werden müssen, muss *Argument* die erforderliche Reihenfolge unterstützen. Parameternamen/Wert-Paare auf der Seite **Aktionskonfiguration** können in einer beliebigen Reihenfolge definiert sein.

Anforderungen an Implementierer

Die externen Prozesse, die für die Aktionen zur erweiterten Zuordnung oder zum Verwalten von Anmeldeinformationen verwendet werden, sind als beliebige Prozesse bzw. Anwendungen definiert, die über eine Befehlszeilenschnittstelle initiiert werden können. Alle erforderlichen oder optionalen Argumente für die Identifizierungserweiterungen oder Aktionserweiterungen müssen ebenfalls in der Befehlszeile mit einer Befehlszeilenschnittstelle festgelegt werden können.

Für Aktionserweiterungen müssen die Implementierer dieselben Funktionen wie in der oben beschriebenen Windows-Erkennungsimplementierung unterstützen. Benutzername, Kennwort, Benutzerdefiniert 1, Benutzerdefiniert 2 und Altes Kennwort können an die ausführbare Datei übergeben werden.

Für Identifizierungserweiterungen und Aktionserweiterungen ist der Implementierer für Folgendes verantwortlich:

- Bereitstellen aller ausführbaren Dateien, Supportmodule und Dateien zur Unterstützung der Erweiterung auf dem Agentcomputer
- Verwalten aller bereitgestellten Module
- Hinzufügen aller festgelegten Registrierungseinträge auf dem Agentcomputer
- Sicherstellen der Eindeutigkeit von Erweiterungsnamen in ihren Domänen

Das empfohlene Benennungsschema für Erweiterungen ist ein umgekehrtes Domänenbenennungsschema (z. B. com.citrix.cpm.ext4).

Aktivieren der Protokollierung

Um das Debugtracing für die Agentsoftware zu aktivieren, muss die Registrierung geändert werden.

Der Name des Registrierungsschlüssels und die zugeordneten Schlüssel befinden sich unter:

[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix \MetaFrame Password Manager\Log]

In der folgenden Tabelle werden die Schlüsselwertmerkmale definiert.

Taste	Typ	Wert
Enabled	REG_DWORD	Standardwert ist 0. 0: deaktiviert 1: aktiviert
Filter	REG_DWORD	Bitmaske, die festlegt, welche Protokolleinträge erstellt werden 0x00000001: Windows-Anwendungsflag zum Protokollieren von Identifizierungs-erweiterungsfehlern 0x00000004: Windows-Kennworteintrag zum Protokollieren von Aktionserweiterungsfehlern
MaxSizeInBytes	REG_DWORD	Maximale Größe der Protokolldatei in Bytes. Der theoretische Höchstwert kann 4 GB (2^32) sein. Standardwert: 819200

Die Protokolldateidaten werden in einer Datei sso_<Benutzername>.log in folgendem Verzeichnis gespeichert:

```
C:\Documente und Einstellungen
\<Benutzername>\Anwendungsdaten\Citrix\MetaFrame Password Manager
```

Virtuelle Tastencodes für Host- und Windows-Anwendungen

In diesem Anhang finden Sie eine Tastencodereferenz für Windows- und Hostanwendungen, u. a.:

- Codes für VTabKeyN (Windows)
- Codes für VirtualKeyCode (Windows) und VKEY (Windows)
- Virtuelle Tastencodes für HLLAPI-kompatible Terminalemulatoren

Codes für VTabKeyN (Windows)

Erstellen Sie mit den folgenden Kennungen eine Tastencodefolge für Windows.

Code	Beschreibung
\`DELAY=N\`	N ist die Anzahl der Millisekunden für die Verzögerung
\`VKEY=N\`	N ist der virtuelle Tastencode, der gesendet wird

Beispiel: Senden von Tabulatortaste, Ende-Taste, Leertaste, einer Verzögerung von 1,5 Sekunden, Benutzername für Anmeldung, Leertaste, Benutzername/ID, Pos1, Verzögerung von 0,35 Sekunden, Tabulatortaste und Kennwort:

```
VTabKey1=`VKEY=9``VKEY=35` `DELAY=1500`Logon
username`VKEY=32`VTabKey2=`VKEY=36``DELAY=350``VKEY=9`
```

Codes für VirtualKeyCode (Windows) und VKEY (Windows)

Mit diesen Codes werden bei der Konfiguration von Anmeldungen an Hostanwendungen bestimmte Tastatureingaben an Felder in Anmelde- oder Kennwortänderungsformularen gesendet.

Taste	Code	Taste	Code	Taste	Code	Taste	Code
Pause	3	5	53	V	86	F5	116
Rücktaste	8	6	54	W	87	F6	117
Tab	9	7	55	X	88	F7	118
Entf	12	8	56	J	89	F8	119
Eingabe	13	9	57	Z	90	F9	120
Umschalt	16	A	65	Links (Fenster)	91	F10	121
Strg	17	B	66	Rechts (Fenster)	92	F11	122
ALT-Taste	18	C	67	Num 0	96	F12	123
Feststelltaste	20	V	68	Num 1	97	F13	124
Esc	27	E	69	Num 2	98	F14	125
Leertaste	32	F	70	Num 3	99	F15	126
Bild Auf	33	G	71	Num 4	100	F16	127
Bild Ab	34	H	72	Num 5	101	F17	128
Ende	35	I	73	Num 6	102	F18	129
Pos1	36	J	74	Num 7	103	F19	130
Links	37	K	75	Num 8	104	F20	131
Auf	38	L	76	Num 9	105	F21	132
Rechts	39	M	77	Sternchen (*)	106	F22	133
Nicht bereit	40	N	78	Plus (+)	107	F23	134
Druck	44	O	79	Minus (-)	109	F24	135
Hilfe	47	Z	80	Punkt (.)	110	Num	144
0	48	Q	81	Strich (/)	111	Rollen	145
1	49	R	82	F1	112	Linke Umschalt-Taste	160
2	50	S	83	F2	113	Rechte Umschalttaste	161
3	51	T	84	F3	114	Linke Strg-Taste	162
4	52	U	85	F4	115	Rechte Strg-Taste	163

Virtuelle Tastencodes für HLLAPI-kompatible Terminalemulatoren

Zeichen/Befehl	Code	Zeichen/Befehl	Code	Zeichen/Befehl	Code
Alt Cursor	@$	Lokaler Druck	@P	PF12/F12	@c
Rücktaste	@<	Zurücksetzen	@R	PF13/F13	@d
@	@@	Umschalt	@S	PF14/F14	@e
ALT-Taste	@A	Dup	@S @x	PF15/F15	@f
Feld -	@A @-	Feldmarkierung	@S @y	PF16/F16	@g
Field +	@A @+	Tabulatortaste (rechte Tabulaturtaste)	@T	PF17/F17	@h
Feld beenden	@A @E	Cursor Auf	@U	PF18/F18	@i
Alt Cursor	@$	Cursor Ab	@V	PF19F19	@j
Eingabe entfernen	@A @F	Cursor links	@L	PF20/F20	@k
Systemabfrage	@A @H	Cursor rechts	@Z	PF21/F21	@l
Einfügen umschalten	@A @I	Bild auf	@u	PF22/F22	@m
Cursorauswahl	@A @J	Bild ab	@v	PF23/F23	@n
Achtung	@A @Q	Ende	@q	PF24/F24	@o
Druck	@A @T	Pos1	@0	PA1	@x
Hexadezimal	@A @X	PF1/F1	@1	PA2	@y
Befehl/Funktionstast e	@A @Y	PF2/F2	@2	PA3	@z
Druck (PC)	@A @t	PF3/F3	@3	PA4	@+
Rücktaste/Linke Tabulatortaste	@B	PF4/F4	@4	PA5	@%
Entf	@C	PF5/F5	@5	PA6	@&
Löschen	@D	PF6/F6	@6	PA7	@’

Zeichen/Befehl	Code	Zeichen/Befehl	Code	Zeichen/Befehl	Code
Eingabe	@E	PF7/F7	@7	PA8	@(
EOF löschen	@F	PF8/F8	@8	PA9	@)
Hilfe	@H	PF9/F9	@9	PA10	@*
Einfügen	@I	PF10/F10	@a		
Neue Zeile	@N	PF11/F11	@b		